



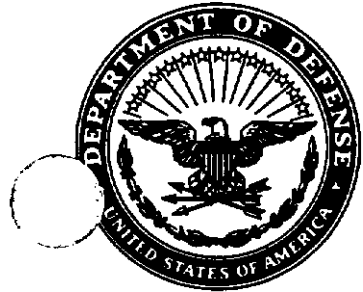
INFORMATION

SECURITY

PROGRAM

January 1997

**THE ASSISTANT SECRETARY OF DEFENSE FOR
COMMAND, CONTROL, COMMUNICATIONS, AND
INTELLIGENCE**



ASSISTANT SECRETARY OF DEFENSE
WOO DEFENSE PENTAGON
WASHINGTON, DC 20301-6000



January 14, 1997

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

FOREWORD

This Regulation is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program, " December 13, 1996. It prescribes procedures for implementation of Executive Order 12958, "Classified National Security Information, " April 20, 1995, within the Department of Defense.

DoD 5200.1-R, "DoD Information Security Program, " June 1986, is hereby canceled.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Uniformed Services University of the Health Sciences, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components") .

This Regulation is effective immediately and is mandatory for use by all the DoD Components. The Heads of the DoD Components may issue implementing instructions when necessary to provide for internal administration of this Regulation within their respective Components.

Send recommended changes to this Regulation through channels to:

Principal Director, Information Warfare, Security and
Counterintelligence
Office of the Assistant Secretary of Defense
Command, Control, Communications, and Intelligence
6000 Defense Pentagon
Washington, DC 20301-6000

The DoD Components may obtain copies of this Regulation through their own publication channels. This Regulation will be published in Title 32, Code of Federal Regulations (CFR), Part



159. The CFR is available in all Government Depository Libraries. Federal Agencies and the public may obtain copies of this Regulation from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. /

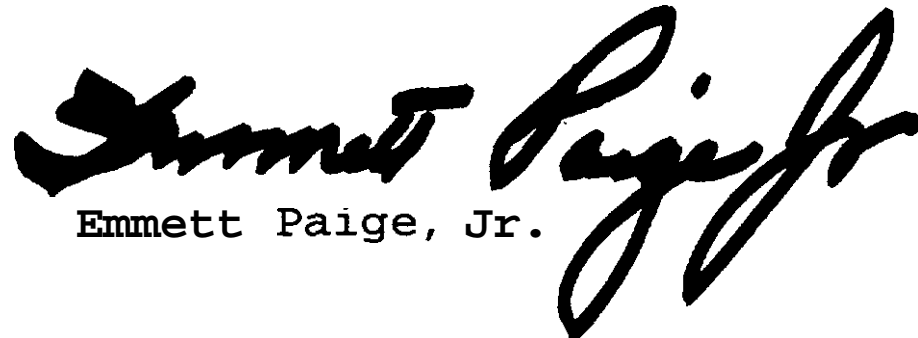

Emmett Paige, Jr.

TABLE OF CONTENTS

	<u>Page</u>
Foreword	i
Table of Contents	iii
CHAPTER 1: POLICY AND PROGRAM MANAGEMENT	
Section 1: Policy	
1-100 Purpose and Scope	1-1
1-101 Policies	1-1
Section 2: Program Management	
1-200 Department of Defense	1-2
1-201 DoD Components	1-2
1-202 Senior Agency Officials	1-2
Section 3: Special Types of Information	
1-300 Restricted Data	1-3
1-301 Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information	1-3
1-302 Special Access Program Information	1-3
1-303 North Atlantic Treaty Organization and Other Foreign Government Information	1-3
Section 4: Exceptional Situations	
1-400 Military Operations	1-3
1-401 Waivers to Requirements	1-3
Section 5: Corrective Actions and Sanctions	
1-500 General	1-4
1-501 Sanctions	1-4
1-502 Reporting of Incidents	1-4
Section 6: Reporta	
1-600 Reporting Requirements	1-4
Section 7: Self-Inspection	
1-700 Self-Inspection	1-5
CHAPTER 2: ORIGINAL CLASSIFICATION	
Section 1: General Provisions	
Section 2: Original Classification Authority	
2-200 Policy	2-1
2-201 Delegation of Authority	2-1

	<u>Page</u>
2-202 Required Training	2-1
Section 3: The Original Classification Process	
2-300 Overview	2-2
2-301 Eligibility for Classification	2-2
2-302 Possibility of Protection	2-2
2-303 The Decision to Classify	2-2
2-304 Level of Classification	2-2
2-305 Duration of Classification	2-3
2-306 Communicating the Decision	2-3
Section 4: Special Considerations	
2-400 Compilation	2-3
2-401 The Acquisition Process	2-3
2-402 Limitations and Prohibitions	2-3
Section 5: Security Classification and/or Declassification Guides	
2-500 Policy	2-4
2-501 Content	2-4
2-502 Approval, Distribution and Indexing	2-4
2-503 Review, Revision and Cancellation	2-4
Section 6: Information from Private Sources	
2-600 Policy	2-5
2-601 Classification Determination	2-5
2-602 Patent Secrecy Act	2-5
CHAPTER 3: DERIVATIVE CLASSIFICATION	
Section 1: Policy and General Requirements	
3-100 The Nature of the Process	3-1
3-101 Authority and Responsibility	3-1
3-102 Policy	3-1
Section 2: Procedures	
3-200 General	3-1
3-201 Special Cases	3-2
CHAPTER 4: DECLASSIFICATION AND REGRADING	
Section 1: General	
4-100 Policy	4-1
4-101 Declassification Systems	4-1
4-102 Declassification Authority	4-1
4-103 Exceptions	4-1
Section 2: Declassification Decisions by Original Classifiers	
4-200 Requirement	4-1
4-201 The “Ten-Year Rule”	4-1

	<u>Page</u>
4-202 Exemption from the 10 Year Rule	4-2
4-203 Extension of Ten-Year Declassification Periods	4-2
 Section 3 : Automatic Declassification at 25 Years	
4-300 The Automatic Declassification System	4-2
4-301 Exemption of Specific Information	4-3
 Section 4: Mandatory Review for Declassification	
4-400 General	4-4
4-401 Responsibilities and Procedures	4-4
 Section 5: Systematic Review for Declassification	
4-500 General	4-5
 Section 6: Downgrading	
4-600 Purpose and Authority	4-5
4-601 Downgrading Decisions During Original Classification	4-5
4-602 Downgrading at a Later Date	4-5
 Section 7: Upgrading	
4-700 General	4-5
 Section 8: Foreign Government Information	
4-800 Policy and Procedures	4-6
4-801 Communications with Foreign Governments	4-6
 Section 9: Challenges to Classification	
4-900 Classification Challenges	4-6
 CHAPTER 5: MARKING	
 Section 1: General Provisions	
5-100 Marking and Designation Rules	5-1
5-101 Exceptions	5-1
5-102 Marking Classified Documents and Other Material	5-1
 Section 2: Specific Markings on Documents	
5-200 Overall Classification Marking	5-2
5-201 Agency, Office of Origin, and Date	5-2
5-202 Source(s) of Classification	5-2
5-203 Reason for Declassification	5-2
5-204 Declassification Instructions	5-3
5-205 Downgrading Instructions	5-5
5-206 Identification of Specific Classified Information	5-5

	<u>Page</u>
5-207 Page Marking	5-6
5-208 Special Control and Similar Notices	5-6
 Section 3: Marking Special Types of Documents	
5-300 Documents With Component Parts	5-7
5-301 Transmittal Documents	5-7
5-302 Classification by Compilation	5-7
5-303 Translations	5-8
5-304 Information Transmitted Electronically	5-8
5-305 Documents and Material Marked for Training Purposes	5-8
5-306 Files, Folders, and Groups of Documents	5-8
5-307 Printed Documents Produced by AIS Equipment	5-8
 Section 4: Marking Special Types of Materials	
5-400 General Policy Statement	5-8
5-401 Blueprints, Schematics, Maps, and Charts	5-9
5-402 Photographs, Negatives, and Unprocessed Film	5-9
5-403 Slides and Transparencies	5-9
5-404 Motion Picture Films and Videotapes	5-9
5-405 Sound Recordings	5-9
5-406 Microforms	5-9
5-407 Removable AIS Storage Media	5-9
5-408 Fixed and Internal AIS Storage Media	5-10
5-409 Standard Form (SF) Labels	5-10
5-410 Intelligence Information	5-10
 Section 5: Changes in Markings	
5-500 Downgrading and Declassification in Accordance with Markings	5-10
5-501 Downgrading and Declassification Earlier Than Scheduled	5-11
5-502 Upgrading	5-11
5-503 Posted Notice on Bulky Quantities of Material	5-11
5-504 Extensions of Duration of Classification	5-11
 Section 6: Remarketing and Using Old Classified Material	
5-600 Old Markings Can Remain	5-11
5-601 Earlier Declassification and Extension of Classification	5-11
 Section 7: Foreign Government Information/Equivalent U.S. Classification Designation	
5-700 General	5-12
5-701 Marking NATO Documents	5-12
5-702 Marking Other Foreign Government Documents	5-12
5-703 Marking of Foreign Government and NATO Information in DoD Documents	5-12
5-704 Marking for Transfer to Archives	5-13

	<u>Page</u>
CHAPTER 6: SAFEGUARDING	
Section 1: Control Measures	
6-100 General	6-1
6-101 Working Papers	6-1
Section 2: Access	
6-200 Policy	6-1
6-201 Access by Persons Outside the Executive Branch	6-1
6-202 Visits	6-3
Section 3: Safeguarding	
6-300 General Policy	6-3
6-301 Care During Working Hours	6-3
6-302 End-of-Day Security Checks	6-3
6-303 Emergency Planning	6-3
6-304 Telephone Conversations	6-4
6-305 Removal of Classified Storage Equipment	6-4
6-306 Residential Storage Arrangements	6-4
6-307 Classified Meetings and Conferences	6-4
6-308 U.S. Classified Information Located in Foreign Countries	6-5
6-309 Information Processing Equipment	6-5
Section 4: Storage	
6-400 General Policy	6-6
6-401 Standards for Storage Equipment	6-6
6-402 Storage of Classified Information	6-6
6-403 Procurement of New Storage Equipment	6-7
6-404 Equipment Designations and Combinations	6-7
6-405 Repair of Damaged Security Containers	6-8
6-406 Maintenance and Operating Inspections	6-9
Section 5: Reproduction of Classified Material	
6-500 Policy	6-9
6-501 Approval for Reproduction	6-9
6-502 Control Procedures	6-9
Section 6: Foreign Government Information	
6-600 General	6-10
6-601 Foreign Government Top Secret, Secret and Confidential Information	6-10
6-602 Foreign Government Restricted Information Provided in Confidence	6-10
6-603 Third-Country Transfers	6-10
6-604 Storage	6-10
Section 7: Disposition and Destruction of Classified Material	
6-700 Policy	6-11
6-701 Methods and Standards	6-11

	<u>Page</u>
Section 8: Alternative or Compensatory Control Measures	
6-800 General	6-11
6-801 Special Access Controls	6-12
CHAPTER 7: TRANSMISSION AND TRANSPORTATION	
Section 1: Methods of Transmission or Transportation	
7-100 Policy	7-1
7-101 Top Secret Information	7-1
7-102 Secret Information	7-1
7-103 Confidential Information	7-2
7-104 Transmission of Classified Material to Foreign Governments	7-3
7-105 Shipment of Freight	7-3
Section 2: Preparation of Material for Transmission	
7-200 Envelopes or Containers	7-3
7-201 Addressing	7-4
Section 3: Escort or Hand-Carrying of Classified Material	
7-300 General Provisions	7-4
7-301 Documentation	7-5
7-302 Hand-carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft	7-5
CHAPTER 8: SPECIAL ACCESS PROGRAMS	
8-100 Policy	8-1
8-101 SAP Procedures	8-1
8-102 Control and Administration	8-2
8-103 Establishment of DoD SAPS	8-2
8-104 Reviews of SAPS	8-5
8-105 Annual Reports and Revalidation	8-6
8-106 Interim Reports	8-6
8-107 Changes in Classification	8-6
8-108 Termination and Transitioning of SAPS	8-7
CHAPTER 9: SECURITY EDUCATION AND TRAINING	
Section 1: Policy	
9-100 General Policy	9-1
9-101 Methodology	9-1
Section 2: Initial Orientation	
9-200 Cleared Personnel	9-1
9-201 Uncleared Personnel	9-2
Section 3: Special Requirements	
9-300 General	9-2

	<u>Page</u>
9-301 Original Classifiers	9-2
9-302 Declassification Authorities Other Than Original Classifiers	9-2
9-303 Derivative Classifiers, Security Personnel and Others	9-2
9-304 Others	9-3
 Section 4: Continuing Security Education/Refresher Training	
9-400 Continuing Security Education	9-3
9-401 Refresher Training	9-3
 Section 5: Termination Briefings	
9-500 General	9-4
 Section 6: Program Oversight	
9-600 General	9-4
 CHAPTER 10: ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION	
10-100 Policy	10-1
10-101 Reporting	10-1
10-102 Inquiry/Investigation	10-2
10-103 Results of the Inquiry/Investigation	10-2
10-104 Verification, Reevaluation, and Damage Assessment	10-3
10-105 Debriefings in Cases of Unauthorized Access	10-3
10-106 Management and Oversight	10-4
10-107 Additional Investigation	10-4
10-108 Unauthorized Absences	10-4
 APPENDIX A: REFERENCES	A-1
 APPENDIX B: DEFINITIONS	B-1
 APPENDIX C: CONTROLLED UNCLASSIFIED INFORMATION	c-1
 APPENDIX D: SPECIAL PROCEDURES FOR USE IN SYSTEMATIC AND MANDATORY REVIEW OF CRYPTOLOGIC INFORMATION	D-1
 APPENDIX E: CONTROL OF DISSEMINATION OF INTELLIGENCE INFORMATION (to be provided at a later date)	E-1
 APPENDIX F: EQUIVALENT FOREIGN SECURITY CLASSIFICATIONS	F-1
 APPENDIX G: PHYSICAL SECURITY STANDARDS	G-1
 APPENDIX H: TRANSMISSION TO FOREIGN GOVERNMENTS	H-1
 APPENDIX I: SPECIAL ACCESS PROGRAM DOCUMENTATION	I-1

CHAPTER 1

POLICY AND PROGRAM MANAGEMENT

Section 1

Policy

1-100 Purpose and Scope

a. This Regulation implements Executive Order 12958, Classified National Security Information, and associated OMB directives within the Department of Defense. It applies to all Components of the Department of Defense. It establishes the Department of Defense Information **Security** Program to promote proper and effective classification, protection and downgrading of **official** information requiring protection in the interest of the national security. It also promotes the declassification of information no longer requiring such protection.

b. There is information, other than classified information, that has been determined to require some type of protection or control. This information is generally known as “controlled unclassified information.” Guidance concerning the protection or controls required for such information may be found in a number of DoD Directives, Regulations and Instructions. However, since classified information and controlled unclassified information often exist **side-by-side** in the work environment, often in the same document, the essence of available guidance pertaining to controlled unclassified information has been captured in Appendix C of this Regulation. The purpose of the Appendix is to provide the user, to the extent possible, a single source document for guidance concerning both classified and controlled unclassified information.

1-101 Policies

a. All personnel of the Department of Defense are personally and individually responsible for providing proper protection to classified information under their custody and control. **All officials** within the Department of Defense who hold command, management, or supervisory positions have specific, **nondelegable** responsibility for the quality of implementation and management of the Information Security Program within their areas of responsibility. Management of classified information **shall** be included as a critical element or item to be evaluated in the rating of original classification authorities, security managers or specialists, and other personnel whose

duties primarily involve the creation or handling of classified information.

b. Except for information subject to the Atomic Energy Act of 1954 (as amended), Executive Order 12958 and this Regulation provide the only basis for application of security classification to information within the Department of Defense.

c. Information shall be classified only when necessary in the interest of national security, and shall be declassified as soon as is consistent with the requirements of national security.

d. Information shall not be reclassified after it has been declassified and **officially released** to the public by proper authority.

e. Persons shall be allowed access to classified information only if they (1) possess a valid and appropriate security clearance, (2) have executed an appropriate non-disclosure agreement, and (3) have a valid need for access to the information to perform a lawful and authorized governmental function. DoD Regulation 5200.2-R contains detailed guidance on personnel security investigation, adjudication and clearance.

f. Classified information shall be protected at **all** times. See Chapters 6 and 7 of this Regulation.

g. Classified information shall be maintained only when it is required for effective and efficient operation of the organization or its retention is required by law or regulation.

h. Classified documents and material that constitute permanently valuable records of the Government shall be maintained and disposed of in accordance with DoD Directive 5015.2. Other classified material shall be destroyed in accordance with Chapter 6 of this Regulation.

i. Special Access Programs **shall** be created, continued, managed, and discontinued in conformance with Chapter 8 of this Regulation.

Section 2

Program Management

1-200 Department of Defense

The Secretary of Defense has designated the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (**ASD(C3I)**) as the senior agency official responsible for direction and administration of the Information Security Program for the Department of Defense. The Under Secretary of Defense for Policy (**USD(P)**) has been designated as the senior official responsible for administering that portion of the DoD Information Security Program pertaining to Special Access Programs (SAPS), the National Disclosure Policy (**NDP**), foreign government (including NATO) information, and security **arrangements** for international programs. These officials shall perform those functions specified in subsection 5.6(c) of Executive Order 12958 and appropriate implementing directives for the Department of Defense.

1-201 DoD Components

The head of each DoD Component shall:

- a. Appoint a senior agency official to be responsible for direction and administration of the program within the Component. (The Component head may designate a separate senior **official** to be responsible for overseeing Special Access Programs within the Component, if necessary.);
- b. Commit necessary resources to the effective implementation of the Information Security Program; and
- c. Establish procedures to ensure that the head of each activity within the Component that creates, handles or stores classified information appoints an official to serve as security manager for the activity, to provide proper management and oversight of the activity's Information Security Program. Persons appointed to these positions shall be provided training as required by Chapter 9 of this regulation.

1-202 Senior Agency Officials

The senior agency official appointed in each Component in accordance with paragraph 1-201 a., above, shall:

- a. Oversee the Component's Information Security Program;
- b. Promulgate (or cause to be promulgated) implementing directives as necessary for program implementation;
- c. Establish and maintain a security education program as required by Chapter 9 of this Regulation;
- d. Establish and maintain an ongoing **self-**inspection program, to include periodic review and assessment of the Component's classified products;
- e. Establish procedures to prevent unauthorized access to classified information;
- f. Develop special contingency plans, as necessary, for the safeguarding of classified information used in or near hostile or potentially hostile areas;
- g. Ensure that the performance contractor other system used to rate the performance of civilian and military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of (1) original classification authorities, (2) security managers and security specialists, and (3) all other personnel whose duties include significant involvement with the creation or handling of classified information;
- h. Account for the costs associated with the implementation of this Regulation within the Component and report those costs as required; and
- i. Ensure prompt and appropriate response to any request, appeal, challenge, complaint, or suggestion arising out of the implementation of this Regulation within the Component.

Section 3

Special Types of Information

1-300 Restricted Data

Classified information in the custody of the Department of Defense marked as Restricted Data under the Atomic Energy Act of 1954 (as amended) shall be stored, protected, and destroyed as required by this Regulation for other information of a comparable level of security classification. DoD policy and procedures concerning access to and dissemination of Restricted Data within DoD are contained in DoD Directive 5210.2.

1-301 Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information

SCI and COMSEC information shall be controlled and protected in accordance with applicable national policy and DoD Directives and Instructions. Security classification and declassification policies of this Regulation apply to SCI and COMSEC information in the same manner as other classified information except that Appendix D of this Regulation provides special procedures for use in systematic and mandatory review of cryptologic information.

1-302 Special Access Program Information

Information covered by Special Access Programs established in accordance with Chapter 8 of this Regulation shall be classified, declassified, controlled and protected as required in this Regulation and instructions issued by officials charged with management of those programs. The provisions of this Regulation pertaining to classification, declassification and marking apply, without exception, to Special Access Program information unless waivers of specific requirements are obtained in accordance with Section 4 of this Chapter.

1-303 North Atlantic Treaty Organization and Other Foreign Government Information

North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with United States Security Authority for NATO (USSAN) Instruction I-69. Other foreign government information shall be safeguarded as described herein for U.S. information except as specified in Appendix H or as required by treaties or international agreements

Section 4

Exceptional Situations

1-400 Military Operations

The provisions of this Regulation pertaining to accountability, dissemination, transmission, and storage of classified information and material may be modified by military commanders as necessary to meet local conditions encountered during military operations. Military operations include combat and peacekeeping operations as well as other operations involving military deployments. Classified information shall be introduced into combat areas or zones, or areas of potential hostile activity, only as necessary to accomplish the military mission.

1-401 Waivers to Requirements

a. Unless otherwise specified herein, DoD Components shall submit requests for waivers to the

requirements of this Regulation through established channels, to the ASD(C3I) or, for information related to SAPS, foreign government information (including NATO) information, and security arrangements for international programs, to the Under Secretary of Defense (Policy) (USD(P)). The ASD(C3I) and USD(P) shall be responsible for promptly notifying the Director, Information Security Oversight Office of all waivers approved involving E.O. 12958 and its' implementing directives.

b. Requests for waivers shall contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security of approval of the waiver. DoD Components shall maintain documentation regarding approved waivers and furnish such documentation, upon request, to other

agencies with whom classified information or secure facilities are shared.

Section 5

Corrective Actions and Sanctions

1-500 General

Heads of the DoD Components shall establish procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, improper classification of information, violation of the provisions of this Regulation, and incidents that may put classified information at risk of compromise. Such actions shall focus on correction or elimination of the conditions that caused or occasioned the incident.

1-501 Sanctions

a. DoD military and civilian personnel **shall** be subject to sanctions if they knowingly, willfully, or negligently:

(1) Disclose to unauthorized persons information properly classified under this Regulation;

(2) Classify or continue the classification of information in violation of this Regulation;

(3) Create or continue a Special Access Program contrary to the requirements of this Regulation; or

(4) Violate any other provision of this Regulation.

b. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law.

c. In case of demonstration of reckless disregard or a pattern of error in applying the classification standards of this Regulation on the part of a person holding original classification authority, the appropriate official shall, as a minimum, remove the offending individual's original classification authority.

1-502 Reporting of Incidents

Whenever a violation under paragraph 1-501a (1), (2) or (3), above, occurs, the Component Senior Agency Official **shall** promptly notify the **ASD(C3I)** through appropriate channels. The **ASD(C3I)** shall notify the Director, Information Security Oversight Office, as required by paragraph 5.7(e)(2) of Executive Order 12958. If the violation involves Special Access Program , NATO or foreign government information, it shall be promptly reported to the Assistant Deputy to the **USD(P)** for Policy Support, who will be responsible for all further notifications and appropriate coordination.

Section 6

Reports

1-600 Reporting Requirements

a. The **ASD(C3I)** shall establish requirements for the collection and reporting of data necessary to support fulfillment of the requirements of Executive Order 12958 and OMB and Security Policy Board implementing directives. As a minimum, DoD Components shall submit, on a fiscal year basis, a consolidated report concerning the Information Security Program of the Component on Standard Form (SF) 311, "Agency Information Security Program Data," to reach the

Principal Director for Information Warfare, Security and Counterintelligence (**PD(IWS&CI)**), **OASD(C3I)**, by October 20 of each year. SF311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the **OASD(C3I)**. The **OASD(C3I)** shall submit the DoD report (SF311) to the Information Security Oversight Office by October 31 of each year. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

b. The **USD(P)** shall establish requirements for the collection and reporting of data necessary to the proper management of Special Access Programs within the Department.

Section 7

Self-Inspection

1-700 General

Heads of DoD Components shall establish and maintain a self-inspection program based on program needs and the degree of involvement with classified information. **The** purpose of the program shall be to evaluate and assess the effectiveness and efficiency of the Component's implementation of the DoD Information Security Program. Component activities that originate significant amounts of classified information should be inspected at least annually.

CHAPTER 2

ORIGINAL CLASSIFICATION

Section 1

General Provisions

Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure, and that the interests of the national security are best served by applying the safeguards of the Information Security Program to protect it. This

decision may be made only by persons who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information. The decision must be made in accordance with the requirements of this chapter.

Section 2

Original Classification Authority

2-200 Policy

Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials who have been specifically delegated this authority in writing. Delegations of original classification authority shall be **limited** to the minimum required for effective operation of the Department of Defense. The authority shall be delegated only to **officials** who have a demonstrable and continuing need to exercise it.

2-201 Delegation of Authority

a. Information may be originally classified Top Secret only by the Secretary of Defense, the Secretaries of the Military Departments, or those officials who have been specifically delegated this authority in writing by the Secretary of Defense or the Secretaries of the Military Departments.

b. Information may be originally classified Secret or Confidential only by the Secretary of Defense, the Secretaries of the Military Departments, and the senior agency officials appointed by them in accordance with Section 5.6(c) of E.O. 12958 provided those senior agency officials have also been delegated original Top Secret classification authority. Senior Agency Officials of the Military Departments may further delegate original Secret and Confidential classification authority

as necessary to respond to requests received under the provisions of paragraphs c and d. below.

c. Requests for original classification authority for officials serving in OSD and the DoD Components other than the Military Departments **shall** be submitted to the **ASD(C3I)**. These requests will specify the position title for which the authority is requested, provide a brief justification for the request, and be submitted through established organizational channels.

d. Requests for original classification authority shall be granted only when (1) original classification is required during the normal course of operations in the organization, (2) sufficient expertise and information is available to the prospective original classification authority to permit effective classification **decision-making**, (3) the need for original classification cannot be eliminated by issuance of classification guidance by existing original classification authorities, and (4) referral of decisions to existing original classification authorities at higher levels in the chain of command or supervision is not practical.

2-202 Required Training

Persons who have been delegated original classification authority must receive training as required by Chapter 9 of this Regulation before they can exercise the delegated authority.

Section 3

The Original Classification Process

2-300 Overview

In making a decision to originally classify information, designated DoD original classification authorities shall:

- a. Determine that the information is owned by, produced by or for, or is under the control of the U.S. Government;
- b. Determine that the information **falls** within one or more of the categories of information listed in subsection 2-301, below;
- c. Determine that the unauthorized disclosure of the information could be expected to result in damage to the national security and be able to identify or describe the damage;
- d. Select the appropriate level of classification to be applied to the information, based on a judgment as to the degree of damage that could be caused by unauthorized disclosure;
- e. Determine the appropriate declassification instructions to be applied to the information; and
- f. Communicate the classification decision as required by subsection 2-306, below.

2-301 Eligibility for Classification

Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.5 of Executive Order 12958:

- a. Military plans, weapon systems, or operations;
- b. Foreign government information;
- c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- d. Foreign relations or foreign activities of the United States, including confidential sources;
- e. Scientific, technological, or economic matters relating to the national security;

f. United States Government programs for safeguarding nuclear materials or facilities; or

g. **Vulnerabilities** or capabilities of systems, installations, projects or plans relating to the national security.

2-302 Possibility of Protection

The original classification authority must determine that, if classification is applied or reapplied, there is a reasonable possibility that the information can be provided protection from unauthorized disclosure. (See paragraph 2-402d. and e., below.)

2-303 The Decision to Classify

a. The decision to apply classification involves two sub-elements, both of which require the application of reasoned judgment on the part of the classifier. The first is the determination that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security of the United States, and that the damage can be identified or described. It is not necessary for the original classifier to produce a written description of the damage at the time of classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request for release under the Freedom of Information Act.

b., The second step in this decision is to determine the probable operational, technological and resource impact of classification.

c. If there is significant doubt about the need to classify information, it shall not be classified.

2-304 Level of Classification

The original classifier, again using reasoned judgment, must determine which level of classification is to be applied. If there is significant doubt about the appropriate level of classification, the information shall be classified at the lower level.

a. Top Secret **shall** be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

c. Confidential shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

2-305 Duration of Classification

At the time of original classification, the original classifier must make a decision about the length of time

the information shall require the protection of security classification. The specific options available in making this decision are discussed in Chapter 3 of this Regulation.

2-306 Communicating the Decision

An original classification authority who makes a decision to originally classify information is **responsible** for ensuring the decision is effectively communicated to persons who will be in possession of the information. This may be accomplished by issuing classification guidance, discussed in Section 5 of this chapter, or by ensuring that a document containing the information is properly marked to reflect the decision. Marking of classified documents is covered by Chapter 5 of this Regulation.

Section 4

Special Considerations

2-400 Compilation

In unusual circumstances, compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that a. qualifies for classification under this Regulation, and b. is not otherwise revealed by the individual information. Classification by compilation must meet the same criteria in terms of justification as other original classification actions. (See paragraph 5-206c and subsection 5-302, below, for marking requirements.)

2-401 The Acquisition Process

Classification of information involved in the DoD acquisition **process shall** conform to the requirements of DoD Directive 5000.1, DoD Regulation 5000.2-R, and DoD Regulation 5000.2-R as well as this chapter.

2-402 Limitations and Prohibitions

a. Classification may not be used to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; or to restrain competition.

b. Basic scientific research and its results may be classified only if it **clearly** relates to the national security.

c. Classification may not be used to prevent or delay the release of information that does not require protection in the interest of the national security.

d. The reclassification of information which was once classified but was declassified and officially released to the public is prohibited.

e. Information may be classified or reclassified after receipt of a request for it under the Freedom of Information Act, the **Privacy** Act of 1974, or the mandatory review provisions of E.O. 12958 only if it is done on a document-by-document basis with the personal participation or under the direction of the Secretary of Defense or Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, or the senior agency official appointed within OSD or a Military Department in accordance with Section 5.6(c) of E.O. 12958.

f. Information that is a product of nongovernment research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may be classified only as provided in Section 6 of this chapter.

Section 5

Security Classification and/or Declassification Guides

2-500 Policy

A security classification guide shall be issued for each system, plan, program, or project in which classified information is involved.

2-501 Content

a. Security classification guides shall:

(1) Identify specific items, elements or categories of information to be protected;

(2) State the specific classification to be assigned to each item or element of information and, when useful, specify items of information that are unclassified;

(3) Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from automatic declassification;

(4) State a concise reason for classification for each item, element, or category of information that, at a minimum, cites the applicable classification category (**ies**) in Section 1.5 of E.O. 12958 (See subsection 2-304, of this Regulation, above;

(5) Identify any special handling caveats that apply to items, elements, or categories of information;

(6) Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of approval; and

(7) Provide a point-of-contact for questions about the guide and suggestions for improvement.

b. For information exempted from automatic declassification because its disclosure would reveal foreign government information or violate a statute, treaty or international agreement (see subsections 4-202 and 4-301 of this Regulation, below), the guide will identify the government or specify the applicable statute, treaty or international agreement as appropriate.

2-502 Approval, Distribution and Indexing

a. Security classification guides shall be approved personally and in writing by an original classification authority who is authorized to classify information at the highest level established by the guide, and who has

program or supervisory responsibility for the information or the organization's Information Security Program.

b. Security classification guides shall be distributed by the originating organization to those organizations and activities they believe will be derivatively classifying information covered by the guide.

c. One copy of each guide shall be forwarded to the Director of Freedom of Information and Security Review, **Office** of the Assistant to the Secretary of Defense for Public Affairs. Guides that cover **SCI** or Special Access Program information and that contain information that requires special access controls are exempt from this requirement.

d. Two copies of each approved guide (other than those covering **SCI** or Special Access Program information, or guides determined by the approval authority for the guide to be too sensitive for automatic secondary distribution) shall be provided to the Administrator, Defense Technical Information Center (**DTIC**). Each guide furnished to **DTIC** must bear the appropriate distribution statement required by DoD Directive 5230.24.

e. Security classification guides issued under this Regulation will be indexed in DoD 5200.1-I, the DoD Index of Security Classification Guides. Originators of guides shall submit DD Form 2024, "DoD Security Classification Guide Data Elements" to the Administrator, **DTIC**, upon approval of the guide. If the originator determines that listing the guide in DoD 5200.1-1 would be inadvisable for security reasons, issuance of the guide shall be separately reported to the **PD(IWS&CI)**, **OASD(C3I)**, with an explanation of why the guide should not be listed. Special Access Program determinations shall be reported separately to the Director, Special Programs, **ODTUSD(P)PS**. Report Control Symbol **DD-C3I (B&AR) 1418** applies to the reporting requirements of this paragraph,

2-503 Review, Revision and Cancellation

a. Security classification guides shall be reviewed by the originator for currency and accuracy at least once every five years. Changes identified as necessary in the review process shall be promptly made. If no changes are required, the record copy of the guide **shall** be so annotated, with the date of the review.

b. Guides shall be revised whenever necessary to promote effective derivative classification. When a guide is revised or reissued, computation of declassification instructions will continue to be based on the date of original classification of the information, not the date of revision or reissue.

c. Guides shall be canceled only when (1) **all** information specified as classified by the guide has been declassified, or (2) when the system, plan, program, or project has been canceled, discontinued, or removed from the inventory, (3) when a major restructure has occurred as the information is incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification.

Impact of the cancellation on systems, plans, programs, and projects provided to other nations under approved foreign disclosure decisions; and impact of such decisions on existing U.S. classification guides of similar systems, plans, programs or projects shall be considered in the decision. Upon cancellation of a guide, the responsible official shall consider the need for publication of a declassification guide, discussed in subsection 4-102 of this Regulation below.

d. Revision, **reissuance**, review, and cancellation of a guide will be reported as required for new guides in paragraph 2-502e, above. Copies of changes, reissued guides, and cancellation notices will be distributed as required by paragraphs 2-502 b., c. and d., above.

Section 6

Information from Private Sources

2-600 Policy

Information that is a product of contractor or individual independent research and development (**IR&D**) or bid and proposal (**B&P**) efforts conducted without prior access to classified information or **current** access to classified information associated with the specific information in question may not be classified unless:

a. The U.S. Government first acquires a proprietary interest in the information; or

b. The contractor conducting the **IR&D/B&P** requests that the U.S. Government activity place the information under the control of the security classification system without relinquishing ownership of the information.

2-601 Classification Determination

a. The individual or contractor conducting an **IR&D/B&P** effort and believing that information generated without prior access to classified information or current access to classified information associated with the specific information in question may require protection in the interest of national security should safeguard the information and submit it to an appropriate U.S. Government activity for a classification determination.

b. The Government activity receiving such a request shall issue security classification guidance as appropriate if the information is to be classified. If the information is not under that activity's classification

authority, the activity shall refer the matter to the appropriate classification authority or inform the individual or contractor to take that action. The information shall be safeguarded until the matter has been resolved.

c. The activity that holds classification authority over the information shall verify whether the individual or contractor is cleared and has been authorized storage capability. If not, the appropriate contracting authority for the activity shall advise whether clearance action should be initiated.

d. If the individual or contractor refuses to be processed for a clearance and the Government does not acquire a proprietary interest in the information, the information may not be classified.

2-602 Patent Secrecy Act

The Patent Secrecy Act of 1952 provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. See DoD Directive 5535.2. A patent application on which a secrecy order has been imposed **shall** be handled as follows within the Department of Defense:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly.

b. If the patent application does not contain information that warrants classification the following procedures shall be followed:

(1) A cover sheet (or cover letter for transmittal) shall be placed on the application with substantially the following language:

The attached material contains information on which secrecy orders have been issued by the U.S. Patent **Office** after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952, 35 **U.S.C.** 181-188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified **CONFIDENTIAL** (or other classification as appropriate).

(2.) The information shall be withheld from public release; its dissemination within the Department of Defense shall be controlled; the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified material.

c. If filing of a patent application with a foreign government is approved under provisions of the Patent Secrecy Act of 1952 and agreements on interchange of patent information for defense purposes, the copies of the patent application prepared for foreign registration (but only those copies) shall be marked at the bottom of each page as follows:

Withheld under the Patent Secrecy Act of 1952 (35 **U.S.C.** 181-188).

Handle as **CONFIDENTIAL** (or such other level as has been determined appropriate),

CHAPTER 3

DERIVATIVE CLASSIFICATION

Section 1

Policy and General Requirements

3-100 The Nature of the Process

Derivative classification is the process of determining whether information that is to be included in a document or material has been classified and, if it has, ensuring that it is identified as classified information by marking or similar means. Information is derivatively classified whenever it is extracted, paraphrased, restated, or generated in a **new** form. Application of classification markings to a document or other material as directed by a security classification guide or other source material is derivative classification. Simply photocopying or otherwise mechanically reproducing classified material is not derivative classification.

3-101 Authority and Responsibility

Within the Department of Defense, all cleared personnel who generate or create material that should be derivatively classified are responsible for ensuring that the derivative classification is accomplished in accordance with this chapter. No specific delegation of authority is required by persons doing derivative classification. DoD officials who sign or approve derivatively classified documents have principal responsibility for the quality of their derivative classification.

3-102 Policy

All persons performing derivative classification shall:

a. Observe and respect the classification determinations made by original classification authorities. If they believe information to be improperly classified, they will take action as required by subsection 4-900 of this Regulation, below.

b. Apply markings or other means of identification to the derivatively classified material as required by Chapter 5 of this Regulation.

c. Use only authorized sources of instructions about the classification of the information in question. Authorized sources of instructions about classification are security classification guides, other forms of classification guidance, and markings on material from which the information is extracted. The use of only memory or “general rules” about the classification of broad classes of information is prohibited.

d. Use caution when paraphrasing or restating information extracted from a classified source document to determine whether the classification may have been changed in the process.

e. Take appropriate and reasonable steps to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification of information. These steps may include consulting a security classification guide or referral to the organization responsible for the original classification. In cases of apparent conflict between a security classification guide and a classified source document about a discrete item of information, the instructions in the security classification guide shall take precedence.

Section 2

Procedures

3-200 General

a. Derivative classifiers must carefully analyze the material they are classifying to determine what information it contains or reveals and evaluate that information against the instructions provided by the classification guidance or the markings on source documents.

b. Drafters of documents that must be derivatively classified should be encouraged to portion mark their drafts and keep records of the sources they use, to facilitate derivative classification of the finished product.

c. Declassification instructions for derivatively classified documents shall not be automatically copied from source documents. They must be determined as required by Chapter 4, and applied in accordance with Chapter 5 of this Regulation.

d. When material is derivatively classified based on “multiple sources” (more than one security classification guide, classified source document, or combination thereof), the derivative classifier must compile a list of the sources used. A copy of this list must be included in or attached to the file or record copy of the document.

3-201 Special Cases

a. If information is extracted from a document or section of a document classified by compilation, the derivative classifier will consult the explanation on the source **document** to determine the appropriate classification. If that does not provide enough guidance, the

originator of the source document should be contacted for assistance.

b. If the derivative classifier has reason to believe the classification applied to information is inappropriate, the classifier of the source document shall be contacted to resolve the issue. The information **will** continue to be classified as specified in the source document until the matter is resolved.

c. If the activity originating the classified information no longer exists, the activity that inherited the functions of the originating activity is responsible for determining the action to be taken with respect to declassification. If the functions of the originating activity were dispersed to more than one other activity, the inheriting activity (**ies**) cannot be determined or, the functions have ceased to exist, the senior agency official of the DoD Component of which the originating activity was a part, is responsible for determining the action to be taken with respect to classification.

CHAPTER 4

DECLASSIFICATION AND REGRADING

Section 1

General

4-100 Policy

E.O. 12958 provides that “information shall be declassified as soon as it no longer meets the standards for classification” established by the Order. It **further** states that, “in some exceptional cases, . . .the need to protect... information [still meeting these standards] may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified.” It is DoD policy that information shall remain classified as long as a. it is in the best interest of the national security to keep it protected, and b. continued classification is in accordance with the requirements of the E.O. If DoD officials have reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they shall refer the matter to the appropriate Senior Agency **Official** appointed in accordance with Section 5.6(c) of E.O. 12958.

4-101 Declassification Systems

E. O. 12958 established four separate and parallel systems that can bring about the declassification of information: (a) a system requiring the original classifier to decide at the time information is classified when it can be declassified, (b) a system that will cause information of permanent historical value to be automatically declassified on the 25th anniversary of its classification unless specific action is taken to keep it classified, (c) a system for reviewing information for possible declassification upon request, and (d) a process for systematic review of information for possible declassification. The Heads of the DoD Components are responsible for ensuring the establishment and maintenance of declassification programs and/or plans to meet the requirements of this subsection.

4-102 Declassification Authority

a. Information may be declassified and downgraded by the Secretary of Defense, the Secretaries of the Military Departments, those officials who have been delegated Original Classification Authority in accordance with subsection 2-201 of this Regulation, above, and officials who have been delegated

declassification authority in accordance with subsection 4-102b, below. The authority to declassify information extends only to information for which the specific official has classification, program, or functional responsibility.

b. DoD Component heads may designate officials within their organizations to exercise declassification authority over specific types or categories of information. Categories of information may be as broad as **all** information originally classified by **officials** of the DoD Component. Classification authorities may designate members of their staffs to exercise declassification authority over information under their jurisdiction.

c. Persons with declassification authority shall develop and issue declassification instructions to facilitate effective review and declassification of information classified under predecessor Executive Orders. These instructions may be in the form of separate guides, sections of classification guides, memoranda, etc.

d. Declassification authority is not required for simply canceling or changing classification markings in accordance with instructions placed on a document, directions found in a security classification guide or declassification guide, or instructions received from a declassification authority.

e. Special procedures for use in systematic and mandatory review of cryptologic information are at Appendix D.

4-103 Exceptions

None of the provisions of this chapter apply to information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data and Formerly Restricted Data).

Section 2

Declassification Decisions by Original Classifiers

4-24)0 Requirement

Every time a designated original classification authority (OCA) classifies information, he or she must make a determination about the duration for which the classification will continue. This is an essential part of the original classification process.

4-201 The “Ten-Year Rule”

At the time they classify an item of information, original classifiers shall:

a. Attempt to determine a date within ten years from the date of classification upon which the information can be automatically declassified. If that is not possible, they shall:

b. Attempt to determine a specific event, reasonably expected to occur within 10 years, that can be set as the signal for automatic declassification of the information. If that is not possible, they shall:

c. Designate the information as being automatically declassified on a date ten years from the date of its original classification, unless the provisions of subsection 4-202, below, apply.

4-202 Exemption from the 10-Year Rule

If an original classifier has substantial reason to believe that information being originally classified **will** require protection for longer than ten years, he or she may exempt the information from the ten-year maximum duration of classification. This may be done **if**:

a. The unauthorized disclosure of the information could reasonably be expected to cause damage to the national security for a period in excess of 10 years, and

b. The release of the information could reasonably be expected to:

(1) Reveal an intelligence source, method, or activity, or a **cryptologic** system or activity;

(2) **Reveal** information that would assist in the development or use of weapons of mass destruction;

(3) Reveal information that would impair the development or use of technology within a United States weapon system;

(4) Reveal United States military plans, or national security emergency preparedness plans;

(5) Reveal foreign government information;

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years;

(7) Impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized;

(8) Violate a statute, treaty, or international agreement.

4-203 Extension of Ten-Year Declassification Periods.

If information has been assigned a date or event for declassification under the ten-year rule described in subsection 4-201, above, and the original classification authority with jurisdiction over the information has reason to believe longer protection is required, he or she may extend the classification for successive periods not to exceed 10 years consistent with agency records retention schedules. Decisions to extend classification must take into account the potential **difficulty** of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who decide to extend a 10-year declassification date are responsible for notifying holders of the information of the decision.

a. For information in records determined to have permanent historical value, successive extensions may not exceed 25 years from the date of the information's origin unless approved as an exception (see section 3 of this chapter).

b. Information in records not determined to have permanent historical value, may be extended past 25 years. However, provisions of normal records retention and destruction requirements must **be** adhered to. Consult your agency's published retention schedule.

Section 3

Automatic Declassification System At 25 Years

4-300 The Automatic Declassification System

a. Executive Order 12958 established a system for declassification of information in permanently valuable historical records (as defined by Title 44, U.S. Code) 25 years from the date of original classification. This system shall be applied to existing records over a **five**-year period beginning with the effective date of the Order (14 October 1995), and shall apply after that to **all** permanently valuable historical records as they become 25 years old. Only the Secretary of Defense and the Secretaries of the Military Departments may exempt information from this automatic declassification under certain circumstances. Information exempted from automatic declassification at 25 years remains **subject** to the mandatory and systematic declassification review provisions of this Regulation.

b. In accordance with the Executive Order, the Secretary of Defense and the Secretaries of the Military Departments have identified specific **file** series that are exempt from the 25-year automatic declassification, and have notified the President of these exemptions. Information in these file series shall not be subject to this automatic declassification system unless an Agency head specifically decides to remove the series from the exempted category. Information not contained within these file series shall be automatically declassified at 25 years unless **specific** information is exempted by an Agency head in accordance with subsection 4-301, below.

c. By 17 April 2000, the Heads of DoD Components shall ensure the declassification of information which: (1) is contained in records which have permanent historical value under Title 44 of the U.S. Code, (2) has not been exempted from automatic declassification at 25 years, and (3) will reach the 25th anniversary of its classification by that date. Declassification operations will be in accordance with plans submitted to the Director of the Information Security Oversight Office in compliance with Subsection 3.4(e) of E.O. 12958.

d. Information contained in records not determined to be permanently valuable and not scheduled for disposal or retention by the National Archives is not subject to automatic declassification. Agency retention and destruction requirements apply.

4-301 Exemption of Specific Information

a. Within the Department of Defense, classified information not contained in file series exempted from the automatic declassification system may be exempted from declassification only by the Secretary of Defense or Secretary of a Military Department. Such exemptions shall be applicable only to specific information. Information may be exempted only if its release would be expected to:

(1) Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national **security** interests of the United States;

(2) Reveal information that would assist in the development or use of weapons of mass destruction;

(3) Reveal information that would impair U.S. cryptologic systems or activities;

(4) Reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) Reveal actual U.S. military war plans that remain in **effect**;

(6) Reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national **security**, are authorized;

(8) Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) Violate a statute, treaty, or international agreement.

b. The Secretary of Defense, the Secretary of a Military Department, or their designated Senior Agency Official, must notify the Director, Information Security

Oversight Office (IS00) of their intent to exempt information **from** automatic declassification. Information previously exempt in accordance with paragraph 4-300b, above, is excluded. Notification must be received by IS00, acting as the executive secretary of the Interagency Security Classification Appeals Panel (ISCAP), 180 days before the information is scheduled for automatic declassification. The notice shall:

- (1) Describe the specific information to be exempted;
- (2) Explain why the information must remain classified; and
- (3) Provide a specific date or event upon which the information will be declassified. (This requirement is not applicable to information exempt from search and review under the Central Intelligence Agency Information Act).

Section 4

Mandatory Review for Declassification

4-400 General

a. Any individual or organization may request a review for declassification of information classified under **E.O.** 12958 or predecessor orders. Upon receipt of such a **request**, the responsible DoD organization shall conduct a review if:

(1) The request describes the document or material with enough specificity to allow it to be located with a reasonable amount of effort;

(2) The information is not exempt from search and review under the Central Intelligence Agency Information Act; and

(3) The information has not been reviewed for declassification within the preceding two years.

b. Information originated by the incumbent President; the incumbent President's White House **Staff**; committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive **Office** of the President that solely advise and assist the incumbent President is exempt from the provisions of this section.

4-401 Responsibilities and Procedures

a. Heads of the DoD Components shall establish systems for promptly responding to requests for mandatory declassification review. Information reviewed shall be declassified if it no longer meets the standards for classification established by this Regulation. Information that is declassified shall be released to the requester unless withholding is appropriate under

applicable law (for example, the Freedom of Information Act or the Privacy Act of 1974).

b. If documents or material being reviewed for declassification under this Section contain information that has been originally classified by another DoD Component or Government Agency, the reviewing activity shall refer the appropriate portions of the request to the originating organization. Unless the association of that organization with the requested information is itself classified, the DoD Component that received the request may notify the requester of the referral.

c. A DoD Component may refuse to confirm or deny the existence or non-existence of requested information when the fact of its existence or non-existence is properly classified.

d. If the requested information has been reviewed for declassification within the two years preceding the request, the DoD Component will so notify the requester. No further review is required.

e. The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester **shall** be notified of the results of the review and of the right to appeal the denial of declassification. If the requester subsequently files an appeal and the appeal is denied, the requester must be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel.

f. Special procedures for use in mandatory review of cryptologic information are at Appendix D.

Section 5

Systematic Review for Declassification

4-500 General

a. Heads of the DoD Components that have classified information under **E.O.** 12958 or predecessor Orders shall, as permitted by available resources, establish systematic review programs to review for declassification information in the custody of the Component that: (1) is contained in permanently valuable historical records, and (2) is exempt from automatic declassification under Section 3 of this chapter. These efforts will concentrate on records **that**:

(a) Contain information which has been identified by the Information Security Policy Advisory Council **established** under **E.O.** 12958 or similar groups to have significant value for historical or scientific research or for promoting the public welfare, and

(b) Have a reasonable likelihood of being declassified upon review.

b. Special procedures for use in systematic review of cryptologic information are at Appendix D.

Section 6

Downgrading

4-600 Purpose and Authority

Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Information may be downgraded by any official who is authorized to classify or declassify the information. (See subsection 4-102, above.)

4-601 Downgrading Decisions During Original Classification

Downgrading should be considered when original classifiers are deciding on the duration of classification to be assigned. If downgrading dates or events can be identified, they must be specified along with the declassification instruction. Note that downgrading instructions **DO NOT** replace declassification instructions.

4-602 Downgrading at a Later **Date**

Information may be downgraded by any official who is authorized to classify or declassify the information. (See subsection 4-102, above.) The authorized **official** making the downgrading decision shall notify holders of the change in classification.

Section 7

Upgrading

4-700 Upgrading

Classified information may be upgraded to a higher level of classification only by **officials** who have been delegated the appropriate **level** of Original Classification Authority in accordance with Section 2, Chapter 2 of this Regulation. Information maybe

upgraded only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The Original Classification Authority making the upgrading decision is responsible for notifying holders of the change in classification.

Section 8

Foreign Government Information

4-800 Policy and Procedures

Within the Department of Defense, every effort must be made to ensure that foreign government information is not **subject** to downgrading or declassification without the prior consent of the originating government. Foreign government information may exist in two forms:

a. Foreign government information may take the form of foreign documents in the possession of the Department of Defense. If these documents constitute permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification rule, declassification **officials** shall consult with the originating foreign government to determine whether it consents to declassification. If the originating foreign government does not consent, the records shall be processed for exemption from automatic declassification in accordance with subsection 4-301,

above. The agency head shall determine whether exemption categories 6, 9, or both should be applied.

b. Foreign government classified information may also be included within a DoD document. Such documents shall be marked with declassification instructions consistent with subparagraph **5-204c(2)** of this Regulation, below. If these documents are permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification **rule**, the **provisions of paragraph 4-800a., above, apply.**

4-801 Communications with Foreign Governments

DoD officials may consult directly with foreign governments regarding downgrading or declassification of foreign government information or seek assistance from the Department of State. In either case, DoD officials should first consult with the Office of the Deputy to the Under Secretary of Defense (Policy Support) for assistance and guidance.

Section 9

Challenges to Classification

4-900 Classification Challenges

a. If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the classifier of the information to bring about any necessary correction. This may be done informally or by submission of a formal challenge to the classification as provided for in **E.O. 12958**. Informal questioning of classification is encouraged before resorting to formal challenge. Heads of the DoD Components shall establish procedures through which authorized holders of classified information within their organizations may challenge classification decisions, and shall ensure that members of their organization are made aware of the established procedures.

(1) Formal challenges to classification made under this subsection shall include **sufficient** description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification made by DoD personnel should also include the reason why the challenger believes that the information is improperly or unnecessarily classified. The challenge should be unclassified, if possible.

(2) Heads of Components shall ensure that no retribution is taken against any employee for making a challenge to a classification.

b. Heads of DoD Components shall establish procedures for handling challenges to classification received from within and from outside their Components. These procedures shall conform to the following guidelines:

(1) A system shall be established for processing, tracking, and recording formal challenges to classification.

(2) The Component shall provide a written response to the challenge within 60 days. If the Component cannot respond fully to the challenge within 60 days, the challenge must be acknowledged and an expected date of response provided. This acknowledgment must include a statement that, if no response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if

an agency has not responded to an internal appeal within 90 days **of** receipt.

(3) If the challenge is denied, the Component shall advise the submitter of his or her right to appeal the decision to the Interagency Security Classification Appeals Panel.

(4) If a challenge is received concerning information that has been the subject of a challenge within the preceding two years, or which is the subject of **pending** litigation, the Component need not process the challenge. The challenger **shall** be informed of the situation and appropriate appellate procedures.

c. Information that is the subject of a **classification** challenge shall continue to be classified and appropriately safeguarded unless and until a decision is made to declassify it.

CHAPTER 5

MARKING

Section 1

General Provisions

5-100 Marking and Designation Rules

All classified information shall be identified clearly by electronic labeling, designation or marking. If physical marking of the medium containing classified information is not possible, then identification of classified information must be accomplished by other means. The term “marking” is intended to include the other concepts of identification. Classification markings must be conspicuous. Marking is the principal means of informing holders of classified information about specific protection requirements for that information. Marking **and designation** of classified information are the specific responsibility of original and derivative classifiers. Markings and designations serve these purposes:

- a. Alert holders to the presence of classified information.
- b. Identify, as specifically as possible, the exact information needing protection.
- c. Indicate the **level** of classification assigned to the information.
- d. Provide guidance on downgrading (if any) and declassification.
- e. Give information on the source(s) of and reasons for classification of the information.
- f. Warn holders of special access, control, or safeguarding requirements.

5-101 Exceptions

No classification or other security markings may be applied to any article or portion of an article that has appeared in a newspaper, magazine, or other public medium. If such an article is evaluated to see if it contains classified information, the results of the review **shall** be kept separate from the article. However, the article and the evaluation may be **filed** together.

Exceptions to specific marking requirements are included with the discussions of the markings.

5-102 Marking **Classified Documents and Other Material**

a. Classified documents must bear the following markings. Material other than ordinary paper documents must have the same information either marked on it or made immediately available to holders by another means. (Specific requirements for each type of marking are found in Section 2 of this chapter.) Requirements for special types of documents are covered in Section 3. Marking material other than paper documents is covered in Section 4. Required markings are:

- (1) The overall classification of the document.
- (2) The agency, office of origin, and date of the document.
- (3) Identification of the source(s) of classification of the information contained *in the* document and, for originally classified information, a concise reason for classification.
- (4) Declassification instructions, and any downgrading instructions that apply. This requirement does not apply to documents containing Restricted Data (**RD**) or Formerly Restricted Data (**FRD**). This information is not marked with declassification instructions.
- (5) Identification of the specific classified information in the document and its **level** of classification (page markings and portion markings).
- (6) Control notices and other markings that apply to the document.

b. The holder of an improperly marked classified document should contact the document originator to obtain correct markings.

Section 2

Specific Markings on Documents

5-200 Overall Classification Marking

Every classified document must be marked to show the highest classification of information it contains. This marking must be conspicuous enough to alert anyone handling the document that it is classified. The overall classification will be marked, stamped, or **affixed** (with a sticker, tape, etc.) on:

- a. The front cover, if there is one.
- b. The title page, if there is one.
- c. The first page. If the document has no front cover, the first page will be the front page. If it has a cover, the first page is defined as the first page you see when you open the cover. In some documents, the title page and first page may be the same.
- d. The outside of the back cover, if there is one.

5-201 Agency, Office of Origin, and Date

Every classified document must show on the first page, title page or front cover (hereafter referred to as the face of the document), the agency and office that originated it, and the date of origination. This information must be clear enough to allow someone receiving the document to contact the preparing office if questions or problems about classification arise.

5-202 Source(s) of Classification

a. Originally Classified Documents. Every originally classified document must have a “Classified by” line placed on the face of the document that identifies the original classification authority responsible for classification of the information it contains. The original classification authority shall be identified by name or personal identifier and position title. If the information normally included on the “Classified by” line would reveal classified information not evident from the rest of the document, the “Classified by” line should be completed with an unclassified personal identifier that can be traced through secure channels. Example:

CLASSIFIED BY: ASD(C3I)
or
CLASSIFIED BY: S-3, 504 MIB

b. Derivatively Classified Documents.

Derivatively classified documents shall not be marked with a “Classified by” line. Instead, they will be marked “Derived from” and the line completed as follows:

(1) If **all** the information was derivatively classified using a single security classification guide or source document, identify the guide or document on the “Derived from” line. Include the date of the source document or classification guide unless the identification of the classification guide implicitly includes the date. Example:

DERIVED FROM Rpt titled: **XXXX**
dtd _____ or

DERIVED FROM: SCG Pgm _
dtd _____

(2) If more than one security classification guide, source document, or combination of these provided the derivative classification guidance, place “Multiple Sources” on the “Derived from” line. If “Multiple Sources” is placed on the “Derived from” line, a record of the sources must be maintained on or with the **file** or record copy of the document. When feasible, this list should be included with all copies of the document. If the document has a bibliography or reference list, this may be used as the list of sources. Annotate it to distinguish the sources of classification from other references.

c. Combinations of Original and Derivative Classification. If some information was originally classified at the time of preparation of the document and other information was derivatively classified, mark the document with a “Classified by” line and place “Multiple Sources” on the line. (The responsible original classification authority shall be identified by position title as one of the “sources” in the list prepared to be maintained with the file or record copy of the document.)

5-203 Reason for Classification

Each originally classified document shall bear a concise statement of the reason for classification, determined by the original classifier. This shall be included on a line accompanying the “Classified by” and “Declassify on” lines on the face of the document. A citation of the appropriate category of information listed in Section 1.5 of E.O. 12958 will satisfy this requirement. (See subsection 2-301, above, for the list

of categories.) Example

CLASSIFIED BY: **ASD(C3I)**
REASON: Foreign Relations or

REASON: 1.5(d)

Note that this marking is NOT required on derivatively classified documents.

5-204 **Declassification** Instructions

Every classified document (except those containing Restricted Data and Formerly Restricted Data) must be marked on the face of the document with a “Declassify on” line, with instructions concerning the declassification of the information in the document. The “Declassify on” line shall be completed according to the following rules:

a. Originally Classified Documents. If all the classified information in the document is classified as an act of original classification, the original classifier must specify the instruction (a date or event less than or equal to 10 years, or an indication that the information is exempt from the 10-year declassification rule) to be placed on the line. If any of the information in the document has been exempted from the 10-year rule (see subsection 4-202, above), the “Declassify on” line will be completed with an “**X**,” followed by a number or numbers that show the applicable exemption category or categories from paragraph 4-202b, above.
Examples:

CLASSIFIED BY: **ASD(C3I)**
REASON: 1.5(d)
DECLASSIFY ON: X2 or

CLASSIFIED BY: S-3, 504 MIB
REASON: Military Plans
DECLASSIFY ON: 20 Jan 1999 or end of
Engineering/Manufacturing/Development (**EMD**)

b. Permanently Valuable 25-Year-Old Documents Exempted from the 25-Year Rule. Only those permanently valuable 25-year-old documents that are approved as exempted from the 25-year automatic declassification system (see Chapter 4, Section 3) will be marked with the designator, “**25X**,” along with the number of the exemption category. The exemption categories are listed in paragraph 4-301a, above. Unless the information concerns a confidential human source or a human intelligence source, the document must also be marked with the declassification date or event set by the exempting authority. An example would be a document exempted from automatic declassification at 25 years that would reveal information

that would impair U.S. **cryptologic** systems or activities, and that was to be declassified on 25 April 2030 might be marked as follows:

CLASSIFIED BY: **ASD(C3I)**
REASON: **Cryptologic** Systems
DECLASSIFY ON: 25X3 or

CLASSIFIED BY: **ASD(C3I)**
REASON: **Cryptologic** Systems
DECLASSIFY ON: 25X3, 25 Apr 2030

A document that would reveal the identity of a confidential human source would be marked: “Declassify on: 25X1.” These markings shall be applied when the exemption from the 25-year rule is approved. Normally, this will mean replacing an older declassification instruction with the exemption marking. Agencies need not apply a “25X” marking to individual documents contained in a file series exempted from automatic declassification until the individual document is removed from the file.

c. Derivatively Classified Documents. In derivative classification, different declassification instructions may apply to the various items of information in your document. To ensure that all the information in the document is protected for as long as necessary, the MOST RESTRICTIVE declassification instruction that applies to any of the information in the document shall be placed on the “Declassify on” line. Examples:

(1) If all the information in the document has THE SAME declassification instruction assigned, and that instruction is an allowable option under E.O. 12958, place that instruction on the “Declassify on” line. The “allowable options” are a date for declassification, an event for declassification, or an exemption marking. Example:

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 25X3 or

DERIVED FROM: SCG Program_____
DECLASSIFY ON: Source dtd 15 July 1995

(2) If all the information in the document has been extracted from a pre-14 October 1995 document marked “OADR,” place the statement “Source marked OADR” on the “Declassify on” line, along with the date of the source document. (Example: You extract classified information from a document dated 3 June 1992 and marked “OADR.” You mark your document, “Declassify on: Source marked OADR; Date of source: 3 June 1992.”) If there is more than one such source, use the latest date found on any of them. Example:

DERIVED FROM: Cite Source
DECLASSIFY ON: Source marked OADR,
d a t e d

(3) If your document is classified by “multiple sources,” and different declassification instructions apply to information you include, you must determine the MOST RESTRICTIVE declassification instruction that applies to any of that information and place it on your “Declassify on” line. The following procedure applies:

(a) If declassification dates are specified for ALL of the information in the document, place the latest date (the date farthest in the future) on the “Declassify on” line. (Example: Your information is extracted from documents marked for declassification on 20 March 1998, 1 June 2002 and 3 April 2009. Mark your document “Declassify on 3 April 2009.”)

(b) If the sources of classification indicate a combination of a date or dates with an event or events, indicate that declassification should occur on the latest date or the occurrence of the event(s), whichever is later. (Example: One source specifies “Declassify on 3 August 2001”; the other is marked “Declassify on completion of tests.” Mark your derivatively classified document “Declassify on 3 August 2001 or completion of tests, whichever is later.”)

(c) If any of the information in the document does not have a definitive date or event for declassification, you **will** have to determine which marking is most restrictive. The following rules apply:

1 If you are using information classified under E.O. 12065 or earlier Orders, any information with an indefinite declassification is treated as though it is marked “OADR.” (For example, if you are using information classified under E.O. 10964 that indicates “Group 3,” this would be treated as though it is marked “OADR.”) When using several sources of information classified under previous Executive Orders that are marked or treated as “OADR,” the “Source dated” line **will** show the source with the most recent date. (For example, with one “OADR” document dated 2 August 1989 and one marked “Group-3” and dated 3 December 1962, the new document would be marked “Declassify on: Source marked OADR; Source dated 2 August 1989.”) No matter what combination of indefinite declassification instructions and document dates you use as your derivative guidance, you need only find the document with the most RECENT DATE and this will determine what the “Source dated” line is going to be. Whatever the “Declassify on” line indicates will be your “Source marked” line. (If you

have three documents, each marked “OADR,” and with the dates of 2 September 1990, 3 December 1992 and 5 October 1995, the most recent date (5 October 1995) is the “Source dated” line. You would mark your document “Declassify on: Source marked OADR, Source dated 5 October 1995”)

2 Sources marked with E.O. 1295810-year exemption markings require a different approach. With documents marked “X1” through “X8,” complete your “Declassify on” line with the exemption marking found on the sources. (You have two sources you use in making a derivative classification decision. Their declassification instructions are “X1” (14 October 1995) and “X2” (18 October 1995). Your declassification instruction would be “Declassify on: **x2.**”)

3 Sources marked with E.O. 1295825-year exemption markings will normally have definite declassification dates indicated. The exception is information marked “25X1” and concerning the identity of a confidential human source. This information will not have a declassification date, and will always be considered your most restrictive source. Mark your document “Declassify on: 25X1.”

4 With sources having a combination of these types of declassification instructions, you must analyze the combination to determine which is most restrictive. Generally, the most current source document would provide your declassification on line. For example:

<u>Source</u>	<u>Declassify on:</u>
Source 1	OADR dtd April 85
Source 2	17 Mar 99
Source 3	OADR dtd Ott 90

The derived document would be marked as follows:

DERIVED FROM: MULTIPLE SOURCES
DECLASSIFY ON: SOURCE MARKED
OADR DTD OCT 90

This information would be subject to declassification 25 years from the date of its origin, thus the date of the source document should always be **placed** on the declassification instruction line.

If the source information included exemption categories, the same process applies. Example:

<u>Source</u>	<u>Declassify on:</u>
Source I	25X2 (weapons of mass

	destruction)
Source 2	17 March 99
Source 3	X5 (foreign government information)

The derived document would be marked as follows:

DERIVED FROM: MULTIPLE SOURCES
DECLASSIFY ON: X5

The information can be extended in successive ten year increments, therefore, the X5 exemption category becomes the most restrictive declassification guidance.

d. Combinations of Original and Derivative Classification. If the classification of the document is through a combination of original and derivative classification, determine the declassification instruction by following the rules in paragraph 5-204.c, above. Use the instruction supplied by the original classifier as if it came from a source document or classification guide.

5-205 Downgrading Instructions

Downgrading instructions are not required for every classified document, but must be placed on the face of each document to which they apply. Mark the document "Downgrade to Secret on..." and/or "Downgrade to Confidential on..." and add the appropriate date or event. (Note: A downgrading instruction is used in addition to, and not as a substitute for, declassification instructions.) Downgrading instructions shall not be applied to documents containing foreign government information or Restricted Data or Formerly Restricted Data.

5-206 Identification of Specific Classified Information

Every classified document must show, as clearly as is possible, which information in it is classified and at what level. Specific marking of each portion ("parenthetical portion marking") **shall** be used.

a. Each section, part, paragraph, and similar portion of a classified document shall be marked to show the highest level of classification of information it contains, or that it is unclassified. When deciding whether a subportion is included in the term "similar portion," the criterion will be whether the marking is necessary to eliminate doubt about the classification of its contents.

(1) Portions of text shall be marked with the appropriate abbreviation ("TS," "S," "C," or "U"), placed in parentheses immediately before the beginning

of the portion. If the portion is numbered or lettered, place the abbreviation in parentheses between the letter or number and the start of the text.

(a) Portions containing Restricted Data and Formerly Restricted Data shall have abbreviated markings ("**RD**" or "**FRD**") included with the classification marking, for example, "**(S-RD)**." Critical Nuclear Weapon Design Information shall be marked with an "N" in separate parentheses following the portion marking: "**(S-RD)(N)**."

(b) Portions of DoD documents containing foreign government or North Atlantic Treaty Organization (NATO) information **shall** include identification of the foreign classification in the parenthetical marking, for example, "(UK-S)" or "(N-S)." Use the letter "R" to identify NATO or foreign government Restricted information.

(c) The abbreviation "FOUO" is used to designate unclassified portions that contain information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). See Appendix C for details.

(2) Subjects and titles of classified documents **shall** be marked to show their classification. Use the same abbreviations as for other portions, **but** place them in parentheses **after** the subject of title. This is the only exception to the placement rule.

(3) Charts, graphs, photographs, illustrations, figures, drawings, and similar portions of classified documents must be marked to show their classification. Captions or titles of these portions must also be marked.

(a) Charts, graphs, and similar items shall be marked with the unabbreviated classification, or "UNCLASSIFIED," based on the level of classified information they contain or reveal. The marking shall be placed within the chart, graph, etc., or next to the item.

(b) Captions and titles of charts, graphs, etc., shall be marked as required for text portions (see subparagraph 5-206a(1), above). The marking **will** indicate the classification of the caption or title, not of the chart itself. (See also paragraph 5-401, below.)

b. If an exceptional situation makes individual markings of each portion clearly impracticable, a statement may be substituted describing which portions are classified and their level of classification. Such a statement must identify the information as specifically as parenthetical portion marking. For classification by

compilation, the statement required by subsection 5-302, below, meets this requirement. A waiver is not required in these situations.

c. Documents containing information classified by compilation (as described in subsection 2-400, above) shall be marked as follows:

(1) If portions, standing alone, are unclassified, but the document is classified by compilation, mark the portions “(U)” and the document and pages with the classification of the compilation. You must also add an explanation of the classification (see subsection 5-302, below).

(2) If individual portions are classified at one level, but the compilation is a higher classification, mark each portion with its own classification, and mark the document and pages with the classification of the compilation. Cite the explanation for the classification by compilation on the Classified By/Derived From line or with the record copy of the material.

d. Waivers of the requirements of this subsection may be granted only by the Director of the Information Security Oversight Office. Waivers granted before 14 October 1995 by DoD officials are no longer valid. Requests for waivers from DoD Components shall be forwarded to the Principal Director (Information Warfare, Security & Counterintelligence), ODASD(I&S) for submission to the Director, 1S00. Waiver requests for Special Access Programs will be forwarded to the Director, Special Programs, ODTUSD(P)PS, who will then forward them to the Director, 1S00. The waiver request must include the following:

(1) Identification of the information or class of documents for which the waiver is sought;

(2) A detailed explanation of why the waiver should be granted;

(3) The Component’s judgment of the anticipated dissemination of the information or class of documents for which the waiver is sought; and

(4) The extent to which the documents subject to the waiver may be a basis for derivative classification.

5-207 **Page** Marking

a. Each interior page of a classified document (except blank pages) shall be conspicuously marked, top and bottom, with the highest classification of the information on the page. These markings must stand

out from the balance of the information and thus a particular size is not specified. Pages containing only unclassified information shall be marked “UNCLASSIFIED.” Blank interior pages will not be marked.

b. An alternative interior page marking scheme is the same as described above except that each page is marked with the highest classification of information in the document. If this alternative is used, parenthetical portion markings must be used instead of the means specified in paragraph 5-206 b., above.

5-208 **Special Control and Similar Notices**

Besides the following, other notices may be required by other DoD Directives. Unless another Directive prescribes different placement, these additional control notices shall be placed on the face of the document.

a. Restricted Data. Documents containing Restricted Data shall be marked:

“RESTRICTED DATA”

“This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.”

b. Documents containing Formerly Restricted Data, but no Restricted Data, shall be marked:

“FORMERLY RESTRICTED DATA”

“Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954”

c. The Director of Central Intelligence (DCI) establishes policies and procedures for the control of dissemination of intelligence information. The current DCI Directive on this subject is at Appendix E.

d. COMSEC Material

The following marking will be placed on classified COMSEC documents before release to contractors. Apply it when the document is created if release to contractors is likely.

“COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance.”

e. Dissemination and Reproduction Notice-s

Classified information that *is* subject to specific dissemination or reproduction limitations maybe marked with notices such as:

“Reproduction requires approval of originator or higher DoD authority”, or

“Further dissemination only as directed by (insert appropriate office or **official**) or higher DoD authority.”

f. Special Access Program Documents

Special Access Program documentation and information may be identified with the phrase “Special

Access Required” and the assigned nickname, codeword, **trigraph**, or digraph.

g. For **Official** Use Only. See Appendix C for guidance on the marking of For **Official** Use Only information contained in classified documents.

h. Other Special Notices

Other requirements for special markings on Restricted Data and Formerly Restricted Data, intelligence and intelligence-related information, **COMSEC** information, technical documents, NATO-classified information, and other information are found in DoD and other agency directives and publications. Consult the references (Appendix A) for further guidance.

Section 3

Marking Special Types of Documents

5-300 Documents with Component Parts

If a classified document has components likely to be removed and used or maintained separately, each component shall be marked as a separate document. Examples are annexes or appendices to plans, major parts of a report, or reference charts in a program directive. If the entire major component is unclassified, it may be marked on its face, top and bottom, “UNCLASSIFIED,” and a statement added: “All portions of this [annex, appendix, etc.] are Unclassified.” No further markings are required on such a component.

5-301 Transmittal Documents

Transmittals are documents that have classified documents enclosed with or attached to them. An example is a letter with classified enclosures. The transmittal document itself may contain information classified as high or higher than the documents transmitted. More often, though, the transmittal document itself is unclassified or classified at a lower level than the transmitted documents.

a. If the transmittal contains information classified higher than or at the same level as the documents it is transmitting, mark it as you would any other classified document. If any special control notices discussed in subsection 5-208, above, apply to the documents transmitted, place them on the face of the transmittal document.

b. If the information in the transmittal document is unclassified or classified at a lower level than one or more of the attachments or enclosures, mark the

transmittal document as follows:

(1) Mark the face of the transmittal document conspicuously, top and bottom, with the highest classification found in it or any of the documents transmitted. (Example: An unclassified transmittal document has one Secret and two Confidential attachments. Mark the face of the transmittal document “SECRET.”)

(2) Mark the face of the transmittal document to show its status when separated **from** the classified material. Examples include: “UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES,” “UNCLASSIFIED WHEN ATTACHMENT 2 IS REMOVED,” “CONFIDENTIAL UPON REMOVAL OF ENCLOSURES,” or a similar statement.

(3) If any of the special control notices described in subsection 5-208, above, apply to the transmittal document or any enclosures, place them on the face of the transmittal document.

(4) Transmittal documents that are classified standing alone must be marked like other classified documents. Unclassified transmittal documents shall not be portion marked. The marking of classification at the top and bottom of interior pages of an unclassified transmittal document is not necessary.

5-302 Classification by Compilation

When a document consisting of individually unclassified items of information is classified by compilation (see subsection 2-400, above), the overall classification shall be marked conspicuously at the top

and bottom of each page and the outside of the front and back covers (if there are covers). An explanation of the basis for classification by compilation shall be placed on the face of the document or included in the text. Mark the portions in accordance with paragraph 5-206c, above.

5-303 **Translations**

Translations of U.S. classified information into a foreign language shall be marked with the appropriate U.S. classification markings and the foreign language equivalent. (See Appendix F for foreign language classifications.) **They** must also clearly show the United States as the country of origin.

5-304 **Information Transmitted Electronically**

Information transmitted electronically, such as messages to be retained as permanent records, rather than those that are facsimile (FAX) transmissions, must be marked as required by this chapter for any other classified **document**, with the following special provisions:

- a. The first item in the text must be the overall classification of the information.
- b. For information printed by an automated system, overall and page markings may be applied by that system, provided they stand out conspicuously from the text. In older systems, this may be achieved by surrounding the markings with asterisks or other symbols.
- c. A properly completed "Classified by" or "Derived from" line, ("Reason," when appropriate), declassification instructions, and downgrading instructions (when appropriate) must be included in the last line. Declassification and downgrading instructions shall not be used for information containing Restricted Data or Formerly Restricted Data. The abbreviations "CLASS" for "Classified by," "RSN" for Reason," **DECL**" for "Declassify on," "DERV" for "Derived from," and "DNG" for "Downgrade to" may be used.

5-305 **Documents and Material Marked for**

Training Purposes

Documents and material that contain no classified information, but are marked with classification markings for training purposes, must also have a marking which clearly shows that they are actually unclassified. A suitable marking shall be placed on each page of the document, for example, "Unclassified - Marked Classified for Training Only."

5-306 **Files, Folders, and Groups of Documents**

Classified files, folders, and similar groups of documents must have clear classification markings on the outside of the folder or holder. Attaching a **classified** document cover sheet (Standard Forms 703, 704, or 705) to the front of the folder or holder **will** satisfy this requirement. These cover sheets need not be attached when the item is in secure storage.

5-307 **Printed Documents Produced by AIS Equipment**

Because of the volume and nature of the printed products of automated information systems (AISs), special provisions for marking some **AIS-generated** documents are required. These special provisions do not apply to documents produced by AISs that function as word processing systems. Documents produced on these AISs are marked like other documents. **The** exceptional provisions are:

- a. Classification markings on interior pages of **fan-**folded printouts are required. These markings may be applied by the AIS equipment even though they may not meet the normal test of being conspicuous.
- b. Special control notices, identification of classification sources, and downgrading and declassification instructions must either be marked on the face of the document or be placed on a separate sheet of paper attached to the front of the document.
- c. Portions of AIS printouts removed for separate use or maintenance shall be marked as individual documents.

Section 4

Marking Special Types of Materials

5-400 **General Policy Statement**

When classified information is contained in AIS media, audiovisual media, hardware and equipment, or

other media not commonly thought of as documents, the provisions of subsection 5-100, above, must be met in a way that is appropriate to the type of material. The main concern is that holders and users of the material

are clearly warned of the presence of classified information needing protection. The information provided by other markings required by this chapter must also be made available, either on the item or in documentation that accompanies it. Particular exceptions are as noted in subsections 5-401 through 5-408, below.

5-401 **Blueprints, Schematics, Maps, and Charts**

Blueprints, engineering drawings, charts, maps, and similar items not contained in a **classified** document must be marked with their overall classification. The classification marking must be unabbreviated, must be conspicuous, and should be applied top and bottom if possible. **The** legend or title must also be marked to show its classification. An abbreviated marking in parentheses following the legend or title may be used. If the blueprints, maps and other items are large enough that they are likely to be rolled or folded, classification markings must be placed to be visible when the item is rolled or folded. For guidance on marking these items when they are pages of a classified document, see subparagraph 5-206a.(3), above.

5-402 **Photographs, Negatives, and Unprocessed Film**

a. Photographs and negatives must be marked with the overall classification of information they contain. Photographs should be marked on the face, if possible. If this cannot be done, the classification marking may be placed on the reverse side. Other markings required by this chapter shall be placed on photographs along with the classification marking, or will be included in accompanying documentation.

b. Roll negatives and positives, and other film containing classified information must be marked with their overall classification. **This** marking must be placed either on the film itself or on the canister, if one is used. If placed on the film itself, the marking must be placed at the beginning and end of the roll.

5-403 **Slides and Transparencies**

a. Slides and transparencies shall have the overall classification and special control notices (detailed in subsection 5-208, above) marked on the image area of the item and also on the border, holder, or frame. Information on the image area of the item **shall** be portion marked in accordance with subsection 5-206, above. **Other** required security markings may be placed in the image area; on the border, holder, or frame; or in documentation accompanying the item.

b. If a group of slides or transparencies is used together and maintained together as a set, each slide or

transparency must have the classification marking and special control notices on it. The other required security markings may be placed on the first slide or transparency in the set; these markings are not needed on the other slides or transparencies. Slides or transparencies that are permanently removed from a set must be marked as a separate document.

5-404 **Motion Picture Films and Videotapes**

Classified motion picture films and videotapes must be marked with their classification and any appropriate control notices at the beginning and end of the played or protected portion. Other required security markings shall be placed at the beginning of the projected or played portion. Reels and cassettes shall be marked with the overall classification of the item and kept in containers marked with the classification and other required security markings.

5-405 **Sound Recordings**

Sound recordings containing classified information must have an audible statement of their classification at the beginning and end. Reels or cassettes shall be marked with the overall classification of the item and kept in containers marked with the classification and other required security markings.

5-406 **Microforms**

Microfilm, microfiche, and similar media must have their overall classification marked in the image area that can be read or copied. They also must have this marking applied so it is visible to the unaided eye. Other required security markings shall be either placed on the item or included in accompanying documentation.

5-407 **Removable AIS Storage Media**

Removable storage media include magnetic tape reels, disk packs, diskettes, CD-ROMs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes and micro-cassettes, and any other device on which data is stored and which normally is removable from the system by the user or operator. All such devices bearing classified information must be conspicuously marked with the highest level of classification stored on the device and any special control notices that apply to the information using one of the labels specified in subsection 5-409, below. As an exception, in the case of CD-ROMs, the label may be **affixed** to the sleeve or container in which the CD-ROM is stored. Other information normally provided by document markings (e.g., "classified by" and "declassify on" lines) shall be available as follows:

a. If the information is stored in readily accessible format on the device, it does not have to be marked on the outside of the device. As an example, if classified files or documents prepared with a word processor are stored on a floppy diskette, and each file bears its own declassification instructions as entered with the word processor, the diskette does not need to be marked with declassification instructions. **This** should be true with respect to most diskettes containing classified word processing files and documents, even though a few of them may not have all of the prescribed markings.

b. If the required information is not stored in readily accessible format on the device, it must be marked on the outside of the device (normally with a sticker or tag) or placed on documentation kept with the device.

5-408 **Fixed and Internal AIS Storage Media**

System managers shall ensure that **AISs**, including word processing systems, provide for classification designation of data stored in internal memory or maintained on fixed storage media.

5-409 **Standard Form (SF) Labels**

a. If not marked otherwise, AIS storage media and other items covered by this Section must be marked with the following labels:

- (1) SF 706- TOP SECRET
- (2) SF 707- SECRET
- (3) SF 708- CONFIDENTIAL
- (4) SF 709- CLASSIFIED
- (5) SF 710- UNCLASSIFIED
- (6) SF711 - DATA DESCRIPTOR

b. SF711 should be used any time classified AIS storage media are removed from the office in which they were created. There is no intention to require use of SF710 in environments where no classified information is created or used. SF 709 should not be used if the appropriate classification label (SF 708, SF 707, or SF 706) is available.

5-410 **Intelligence Information**

a. Additional security controls and markings are established for the dissemination of intelligence information. Appendix E contains a reprint of the current Director of Central Intelligence Directive **(DCID) 1/7**. The **DCID 1/7** establishes policies, controls and procedures for the dissemination and use of intelligence information and is applicable to classifiers of intelligence information.

b. The DCID eliminates several markings. Refer to the DCID for instructions on marking and releasing procedures for information marked with the following obsolete caveats:

Not Releasable to Foreign Nationals
(NOFORN)

Release to (REL TO)

Warning Notice-Intelligence Sources or
Methods Involved **(WNINTEL)**

Not Releasable to Contractors/Consultants
(NOCONTRACT or NC)

c. Information previously marked NOFORN continues to be non-releasable to foreigners and must be referred to the originator. NOFORN is not authorized for new classification decisions. A limited amount of information will contain the marking US ONLY. This information cannot be shared with any foreign government. As with all disclosure decisions, the National Foreign Disclosure Policies must be adhered to.

Section 5

Changes in Markings

5-500 **Downgrading and Declassification in** Accordance with Markings

a. When a document or item of material is marked for downgrading or declassification on a date or event, the downgrading or declassification is automatic at the specified time unless word to the contrary has been received from the originator or other authority. There

is no requirement to refer the material to the originator on that date for a downgrading or declassification decision. If a holder of the material has reason to believe it should not be downgraded or declassified, he or she shall notify the originator through appropriate administrative channels. The document or material shall continue to be protected at the originally assigned level of classification until the issue is resolved.

b. When a document is declassified automatically in accordance with declassification markings appearing on it, the overall and page markings on the document should be canceled, if practical. For a bulky document, where canceling each page marking is not practical, cancel at least the markings on the cover (if one exists), title page (if one exists), and the **first** page.

c. If a document is downgraded **in accordance with its markings, cancel the old classification markings and substitute the new ones.** As a **minimum, the markings on the cover (if one exists), title page (if one exists), and the first page must be changed.**

5-501 Downgrading and Declassification Earlier Than Scheduled

If a document is declassified or downgraded earlier than indicated by its markings, the rules-for remarking in subsection 5-500, above, must be followed. In addition, place the following information on the document:

a. The date of the downgrading or declassification remarking.

b. The authority for the action (e.g., the identity of the original classifier who directed the action, or identification of the correspondence or classification instruction that required it). When possible, file a copy of the correspondence authorizing the downgrade or declassification with the document.

5-502 Upgrading

If a document is upgraded, all classification markings affected by the upgrading must be changed to the

new markings. Also place the following information on the document:

a. The date of the remarking.

b. The authority for the action (e.g., the identity of the original classifier who directed the action, or identification of the correspondence or classification instruction that required it).

5-503 Posted Notice on Bulk Quantities of Material

If the volume of material involved in a declassification, downgrading, or upgrading action is so large that individually remarking each item would cause serious interference with operations, the custodian may attach a notice to the inside of the storage unit providing the information required by subparagraph 5-500, 5-501, or 5-502, above, whichever applies. When individual documents are removed from the storage unit, they must be marked in the manner prescribed under subsection 5-500, above. If documents are removed to be transferred to another storage unit, they need not be remarked if the new storage unit also has a proper notice posted.

5-504 Extensions of Duration of Classification

If information has been marked for declassification at 10 years from its date of classification and the duration of classification is subsequently extended, the "Declassify on" line shall be changed to show the new declassification instructions, the identity of the OCA or other authority authorizing the extension, and the date of the action. (Example: "Declassify on: Classification extended on 1 Dec. 2000 until 1 Dec 2010 by D. Jones, Ch., Div 5.")

Section 6

Remarking and Using Old Classified Material

5-600 Old Markings Can Remain

Some classified documents and other material are still in use that were marked in accordance with E.O. 12356 and earlier orders. **There** is no need to remark this **material** with the new declassification and downgrading instructions specified by E.O. 12958. If the material is marked for automatic downgrading or declassification on a date or event, downgrade or declassify it in accordance with those markings. If the material is of permanently historical value and does not show a specific declassification date or event, it will be subject to the automatic declassification provisions of E.O. 12958 as it reaches 25 years from its date of

origin.

5-601 Earlier Declassification and Extension of Classification

The requirements for declassification and for extension of classification found in Chapter 4 of this Regulation apply to information classified under E.O. 12356 and earlier Executive orders, as well as to information classified under the current Executive Order.

Section 7

Foreign Government Information/Equivalent U.S. Classification Designation

5-700 General

Classification designations for foreign government information in many cases do not parallel U.S. classification designations. Moreover, many foreign governments and international organizations have a fourth level of classification that generally translates as “Restricted,” and a category of unclassified information that is protected by law in the originating country and is provided on the condition that it will be treated “in confidence.” A table of U.S. and foreign government classification markings is at Appendix F.

5-701 Marking NATO Documents

NATO classified documents (i.e., documents prepared by or for NATO and NATO member nation documents that have been released into the NATO security system and which bear a NATO classification marking) shall be marked in compliance with USSAN Instruction 1-69.

5-702 Marking Other Foreign Government Documents

a. Except as described in subparagraph b., below, other foreign government classified documents shall be marked in English to identify the originating country and the applicable U.S. classification designation. If a classification designation has been applied to a foreign document by the originator, and it is the applicable U.S. English language designation, only the identity of the originating country need be applied to the document. Examples:

(1) A German document marked “**Geheim**” would be marked:

GERMAN SECRET

(2) AUK document marked “**SECRET**” would be marked:

UK SECRET

b. Foreign government documents that are marked with a classification designation which equates to Restricted, and unclassified foreign government documents that are provided to a DoD

Component on the condition that they will be treated “in confidence,” shall be marked to identify the originating government and whether they are Restricted or provided “in Confidence” Additionally, they shall be marked “**CONFIDENTIAL - Modified Handling**” and be protected in accordance with section 6-600, below. Example:

A French document marked “**Diffusion Restreinte**” would be marked:

FRENCH RESTRICTED INFORMATION
Protect as
CONFIDENTIAL-Modified Handling

5-703 Marking of Foreign Government and NATO Information in DoD Documents

a. When used in DoD documents, foreign government information (**FGI**) must be marked to prevent premature declassification or unauthorized disclosure. To satisfy this requirement, U.S. documents that contain foreign government information shall be marked on the cover or first page, “THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION.” In addition, the portions shall be marked to identify the classification level and the country of origin, e.g., (UK-C); (GE-C). If the identity of the foreign government must be concealed, the cover or first page of the document shall be marked, “THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION,” and applicable paragraphs shall be marked FGI together with the appropriate classification (**FGI-S**). The identity of the foreign government shall be maintained with the record copy which must be appropriately protected.

b. The “Derived From” line shall identify the U.S. as well as foreign classification sources. If the identity of the foreign government must be concealed, the “Declassify on” line shall contain the notation, “Originating Agency Determination Required,” or “OADR.” and the identity of the foreign government maintained with the record copy and protected as in paragraph 5-703a., above. A U.S. document marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations

concerning downgrading or declassification shall be submitted through the DoD entity that created the document to the originating foreign government.

c. DoD classified documents that contain extracts of NATO classified information shall be marked as follows on the cover or first page: “THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION.” Portions **shall** be marked to identify the NATO information (e.g., N-S). All other markings prescribed in subsection 5-102, above, are applicable to these documents.

d. When NATO or other foreign government RESTRICTED information is included in otherwise unclassified DoD documents, the following statement shall be **affixed** to the top and bottom of the page containing the information: “This page contains (indicate NATO or country of origin) RESTRICTED information.” The Restricted portions shall be portion marked (e.g., **(NR)**; (UK-R), **(NR)**.” The cover, (or first page, if no cover) of the document shall contain the following statement “This document contains NATO Restricted information not marked for declassification (date of source) and shall be safeguarded in accordance with USSAN 1-69.

5-704 Marking for Transfer to Archives

When classified records are to be **transferred** for storage or archival purposes to the National Archives and Records Administration or to other locations, the records that accompany them shall identify the boxes that contain foreign government documents as well as DoD documents containing foreign government information.

CHAPTER 6

SAFEGUARDING

Section 1

Control Measures

6-100 General

a. Components shall have a system of control measures that ensure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

b. Foreign government information shall be controlled and safeguarded as described in Section 6 of this Chapter.

6-101 Working Papers

Working papers ~~are~~ documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

- a. Dated when created;
- b. Marked with the highest classification of any information contained therein;
- c. Protected in accordance with the assigned classification:
- d. Conspicuously marked "Working Paper" on the first page of the document in letters larger than the text.
- e. Destroyed when no longer needed; and
- f. Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when retained more than 180 days from date of origin or released by the originator outside the activity.

Section 2

Access

6-200 Policy

Except as otherwise provided in subsection 6-201, below, no person may have access to classified information unless that person has been determined to be trustworthy and access is essential to the accomplishment of a lawful and authorized Government purpose. DoD Regulation 5200.2-R contains detailed guidance concerning personnel security investigation, adjudication and clearance. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests with the individual who has

authorized possession, knowledge, or control of the information and not on the prospective recipient.

6-201 Access by Persons Outside the Executive Branch

Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national

security and assurance of the recipient's trustworthiness and need-to-know.

a. Congress. Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with DoD Directive 5400.4. Any DoD employee testifying before a Congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that maybe discussed. Members of Congress by virtue of their elected positions, are not investigated or cleared by the Department of Defense.

b. Government Printing Office (GPO). Documents and material of all classification maybe processed by the GPO, which protects the information in accordance with the DoD/GPO Security Agreement of February 20, 1981.

c. Representatives of the General Accounting Office (GAO). Representatives of the GAO maybe granted access to classified information originated by and in the possession of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoD Directive 7650.1. Certifications of security clearances, and the basis therefor, shall be accomplished pursuant to arrangements between GAO and the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

d. Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that an authorized official within the DoD Component with classification jurisdiction over the information:

(1) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be trustworthy pursuant to paragraph 6-200, above, and DoD 5200.2-R;

(2) Limits such access to specific categories of information over which the DoD Component has classification jurisdiction and to any other category of information for which the researcher obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed

by documents within the scope of the proposed historical research;

(3) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Administration;

(4) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein by execution of a statement entitled, "Conditions Governing Access to Official Records for Historical Research Purposes"; and

(5) Issues an authorization for access valid for not more than 2 years from the date of issuance that may be renewed under regulations of the issuing DoD Component.

e. Former Presidential Appointees. Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, provided that an authorized official within the DoD Component with classification jurisdiction for such information:

(1) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be trustworthy pursuant to subsection 7-100, below;

(2) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed access;

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Administration: and

(4) Obtains the former presidential appointee's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Component or **non-DoD** departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

f. Judicial proceedings. DoD Directive 5405.2 governs the release of classified information in litigation.

g. Other Situations. When necessary in the interests of national security, heads of DoD Components, or their senior agency official, may authorize access by persons outside the Federal Government, other than those enumerated above, to

classified information upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective; and that the recipient can and will safeguard the information from unauthorized disclosure.

6-202 Visits

Heads of DoD Components shall establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. As a minimum, these procedures will include verification of the identity, personnel security clearance, access (if appropriate), and need-to-know for all visitors.

Section 3

Safeguarding

6-300 General Policy

Everyone who has been granted access to classified information is responsible for providing protection to information and material in their possession or control that contains such information. Classified information must be protected at all times either by storage in an approved device or facility or having it under the personal observation and control of an authorized individual. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

6-301 Care During Working Hours

a. Classified material removed from storage shall be kept under constant surveillance of authorized persons. Classified document cover sheets (Standard Forms 703, 704 and 705) will be placed on classified documents not in secure storage.

*

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter and printer ribbons, floppy disks, and other items containing classified information shall be either destroyed immediately after they have served their purpose or protected as required for the level of classified information they contain.

6-302 End-of-Day Security Checks

Heads of activities that process or store classified information shall establish a system of security checks at the close of each working day to ensure that the area is secure. Standard Form 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system **shall** be the securing of **all** vaults, secure rooms, and containers used for the storage of classified material; Standard Form 702, "Security Container Check Sheet," shall be used to record such actions. In addition, Standard Forms 701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity.

6-303 Emergency Planning

a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The **level** of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster, or terrorist activity that might place the information in jeopardy.

b. Planning for the emergency protection (including emergency destruction under no-notice conditions) of classified **COMSEC** material **shall** be developed in accordance with requirements of National Telecommunications Information Systems Security Instruction (NTISSI) 4004.

c. When preparing emergency plans, consideration should be given to:

- (1) Reduction of the amount of classified **material** on hand;
- (2) Storage of less frequently used classified material at more secure locations; and
- (3) Transfer of as much retained classified information to microforms or to removable automated information systems media as possible, thereby reducing its bulk.

6-304 Telephone Conversations

Classified information shall be discussed in telephone conversations only over secure communications circuits approved for transmission of information at the specific level of classification. When discussing classified information on the telephone, the ability of others in the area to overhear what is being said must be considered.

6-305 Removal of Classified Storage Equipment

Storage containers that may have been used to store classified information shall be inspected by properly cleared personnel before removal from protected areas or unauthorized persons are allowed access to them. The inspection should ensure that no classified information remains within the equipment.

6-306 Residential Storage Arrangement

a. Only the Secretary of Defense, the Secretaries of the Military Departments, the Combatant Commanders and the Senior Agency Official of the DoD Component may authorize removal of Top Secret information from designated working areas in off-duty hours for work at home.

b. Heads of DoD Components or their designees may authorize removal of Secret and Confidential information from designated working areas in off-duty hours for work at home. Authority to approve such removal shall not be delegated below the major command or equivalent level.

c. A GSA-approved security container shall be furnished for residential storage. Written procedures shall be developed to provide for appropriate protection of the information, to include a record of the information that is authorized for removal.

6-307 Classified Meetings and Conferences

a. Meetings and conferences that involve classified information present special **vulnerabilities** to unauthorized disclosure. Heads of the DoD Components shall establish specific requirements for protection of classified information at Component conferences, seminars, exhibits, symposia, conventions, training courses, or other such gatherings during which classified information is disseminated. This does not apply to in-house gatherings, routine gatherings of U.S. Government officials, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific government contract, program, or project. Requirements developed shall, as a minimum, include a determination that:

(1) The meeting **will** serve a specific U.S. Government purpose;

(2) The use of other appropriate channels for dissemination of classified information or material are insufficient;

(3) The meeting location will be under the security control of a U.S. Government agency or a U.S. contractor with an appropriate facility security clearance;

(4) Adequate security procedures have been developed and **will** be implemented to minimize risk to the classified information involved;

(5) Classified sessions shall be segregated from unclassified sessions whenever possible; and

(6) Access to the meeting or conference, or *specific* sessions thereof, at which classified information will be discussed or disseminated, will be limited to persons who possess an appropriate security clearance and need-to-know.

(7) Any participation by foreign nationals or foreign representatives complies with the requirements of DoD Instruction 5230.20 and DoD Directive 5230.11; e.g., assurance is obtained, in writing, from the responsible U.S. Government foreign disclosure office(s) that the information to be presented has been cleared for foreign disclosure.

(8) Announcement of the classified meeting shall be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(9) Non-government organizations may assist in organizing and provide administrative support for a classified meeting, but **all** security requirements remain the specific responsibility of the DoD Component sponsoring the meeting.

(10) Procedures must ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by **other** provisions of **this** Regulation. Note taking or electronic recording during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

b. Special requirements apply to meetings, conferences, seminars, and activities other than those described in subparagraph 6-307 a., above, at which **classified** information is to be presented and discussed as follows:

(1) Meetings must be approved by the head of the DoD Component, a person serving at the level of Deputy Assistant Secretary or above **within** OSD, the Director of the Joint Staff, the Directors of the Defense Agencies, or the Senior Agency Officials appointed within the Military Departments in accordance with Section 5.6(c) of E.O. 12958.

(2) A DoD official is appointed by the DoD *Component sponsoring the meeting, to serve as* security manager for the meeting and physical security of the actual site of the classified meeting is established and maintained by U.S. Government personnel. Other U.S. Government organizations or cleared DoD contractors with appropriate facility security clearances may assist with implementation of security requirements under the direction of the appointed security manager.

6-308 U.S. Classified Information Located in Foreign Countries

Except for classified information that has been authorized for release to a foreign government or international organization pursuant to DoD Directive 5230.11, and is under the security control of that government or organization, U.S. classified material may be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. Heads of the DoD Components will prescribe requirements for protection *of* this information, with particular attention to ensuring proper enforcement of controls on release of U.S. classified information to foreign entities. U.S.

classified material in foreign countries shall be stored as described in paragraphs a. through d. **below**. The provisions of Section 4, below, also apply.

a. At a U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel.

c. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

d. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control, provided the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access.

6-309 Information Processing Equipment

The Department of Defense has a variety of **non-**COMSEC-approved equipment *that is used to process* classified information. This includes copiers, facsimile machines, AIS equipment and peripherals, electronic typewriters, word processing systems, and others. Activities must identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures must prescribe the appropriate safeguards to:

a. Prevent unauthorized access to that information.

b. Replace and destroy equipment parts as classified material when the information cannot be removed from them. Alternatively, the equipment may be designated as classified and appropriately protected at the retained information's classification level.

c. Ensure that equipment is inspected by appropriately cleared and technically knowledgeable personnel before the equipment is removed from protected areas.

Section 4

Storage

6-400 General Policy

Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this Regulation represent acceptable security standards. DoD policy concerning the use of force for the protection of classified information is specified in DoD Directive 5210.56. Weapons or sensitive items such as funds, jewels, precious metals or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

6-401 Standards for Storage Equipment

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. DoD Directive 3224.3 describes acquisition requirements for physical security equipment used within the Department of Defense.

6-402 Storage of Classified Information

Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, as follows:

a. Top Secret information shall be stored by one of the following methods:

(1) In a GSA-approved security container with one of the following supplementary controls:

(a) The location that houses the security container shall be subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every two hours;

(c) An Intrusion Detection System (IDS) meeting the requirements of Appendix G with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

(d) Security-In-Depth when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

(2) Modular vault, vault, or a secure room constructed in accordance with Appendix G and equipped with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5 minute alarm response time if it is not. (Other rooms that were approved for the storage of Top Secret in the U.S. may continue to be used.)

(3) New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740.

(4) Under field conditions during military operations, the commander may prescribe the measures deemed adequate to meet the storage standard contained in subparagraphs 6-402a. 1. and 2., above.

b. Secret information shall be stored by one of the following methods:

(1) In the same manner as prescribed for Top Secret information,

(2) In a GSA-approved security container or vault without supplemental controls;

(3) In secure rooms that were approved for the storage of Secret information by the DoD Components prior to October 1, 1995; or

(4) Until October 1, 2002, in a non-GSA - approved container having a built-in combination lock or in a non-GSA approved container secured with a rigid metal lockbar and a GSA-approved padlock with one of the following supplemental controls:

(a) The location that houses the container is subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every four hours; or

(c) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm.

c. Confidential information shall be stored in the same manner as prescribed for Top Secretor Secret information except that supplemental controls are not required.

d. Specialized Security Equipment

(1) The Heads of the DoD Components shall, consistent with this Regulation, delineate the appropriate security measures required to protect classified information stored in containers on military platforms or for classified munitions items.

(2) GSA-approved field safes and special purpose one and two drawer light-weight security containers approved by the GSA are used primarily for storage of classified information in the field and in military platforms. Such containers shall be securely fastened to the structure or under sufficient surveillance to prevent their theft.

(3) GSA-approved map and plan files are available for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

(4) GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information as an alternative to vault requirements described in Appendix G.

e. **Replacement of Combination Locks.** The mission and location of the activity, the classification level and sensitivity of the information, and the overall security posture of the activity determines the priority for replacement of existing combination locks. All system components and supplemental security measures including electronic security systems (e.g., intrusion detection systems, automated entry control subsystems, and video assessment subsystems), and level of operations must be evaluated by the commander when determining the priority for replacement of security equipment. Appendix G, provides a matrix illustrating a prioritization scheme for the replacement of existing combination locks on GSA-approved security

containers and vault doors. Priority 1 requires immediate replacement.

f. Storage areas for bulky material containing Secret or Confidential information may have access openings secured by GSA-approved changeable combination padlocks (Federal Specification FF-P- 110 series) or high security key-operated padlocks (Military Specification MIL-P-43607). Other security measures are required, in accordance with subsection 6-308, above.

(1) When special circumstances exist, Heads of DoD Components may authorize the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

(2) Section 1386 of title 18, United States Code, makes unauthorized possession of keys, key-blanks, keyways or locks adopted by any part of the Department of Defense for use in the protection of conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

6-403 Procurement of New Storage Equipment

a. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by the heads of the DoD Components, with notification to the ASD(C³I).

b. Nothing in this chapter shall be construed to modify existing Federal supply class management assignments made under DoD Directive 5030.47.

6-404 Equipment Designations and Combinations

a. There shall be no external mark revealing the level of classified information authorized to be or actually stored in a given container or vault or to the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol, (e.g. a bar code) on the container for other purposes (e.g. identification and/or inventory purposes) nor from applying decals or stickers required by the Director of Central Intelligence for containers and equipment used to store or process intelligence information.

b. Combinations to Containers and Vaults

(1) Combinations to security containers, vaults and secure rooms shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(a) When placed in use;

(b) Whenever an individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(c) When the combination has **been** subject to possible compromise;

(d) When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

(2) The combination of a container, vault or secure room used for the storage of classified information **shall** be treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the appropriate classification level.

(3) A record shall be maintained for each vault or secure room door, or container used for storage of classified information, showing location of the door or container, and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination who are to be contacted in the event that the vault, secure room, or container is found open and unattended.. Standard Form 700, "Security Container Information," **shall** be used for this purpose.

(4) Access to the combination of a vault, secure room or container used for the storage of classified information **shall** be granted only to those individuals who are authorized access to the classified information to be stored therein or for the purpose of changing combinations or the repair of vaults or security containers..

b. Entrances to secure rooms or areas should be under visual control at all times during duty hours to prevent entry by unauthorized personnel or equipped with electric, mechanical or electromechanical access control devices to limit access during duty hours. Appendix G provides standards for these access control devices; the use of automated systems

described therein is encouraged. Electrically actuated locks (e.g., cypher and magnetic strip card **locks**) do not afford by themselves the required degree of protection for classified information and must not be used as a substitute for the locks prescribed in subsection 6-402, above.

6-405 Repair of Damaged Security Containers

Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination in accordance with DoD 5200.2-R or are continuously escorted while so engaged.

a. With the exception of frames bent through application of extraordinary stress, a GSA-approved security **container** manufactured prior to October 1991 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity if repaired in accordance with Appendix G.

(1) All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced; or

(2) Has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, a replacement lock meeting **FF-L-2740** is used, and the drilled hole is repaired with a tapered, hardened **tool-**steel pin, or a steel dowel, drill bit, or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a shallow recess not less than 1/8 inch nor more than 3/16-inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

b. In the interests of cost efficiency, the procedures identified in paragraph 6-405 .a.(2)., above, should not be used for GSA-approved security containers purchased after October 1991 (distinguished by a silver GSA label with red lettering affixed to the outside of the container control drawer) until it is first determined whether warranty protection still applies. To make this determination, it will be necessary to contact the manufacturer and provide the serial number and date of manufacture of the

container. If the container **is** under warranty, a lock-out will be neutralized using the procedures described in the Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR.

c. Unapproved modification or repair of security containers and vault doors is considered a violation of the container's or door's integrity and the GSA label shall be removed. Thereafter, they may not be used

to protect classified information except as otherwise authorized in this Regulation.

6-406 **Maintenance and Operating Inspections**

Heads of DoD Components shall establish procedures concerning repair and maintenance of classified material security containers and vaults.

Section 5

Reproduction of Classified Material

6-500 **Policy**

Documents and other material containing classified information shall be reproduced only when necessary for accomplishment of the organization's mission or for compliance with applicable statutes or directives. Since reproduction equipment and the reproduction process involve substantial risk, heads of the DoD Components **shall** establish and enforce procedures for reproduction of classified material that limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk.

The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

6-501 Approval for Reproduction

Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs. The DoD Components shall establish procedures that, as a minimum:

a. Ensure compliance with reproduction limitations placed on documents by originators and special controls applicable to Special Access Programs and other special categories of information;

b. Facilitate oversight and control of reproduction of classified material; and.

c. Ensure the expeditious processing of documents in connection with review for declassification.

6-502 **Control Procedures**

The DoD Components shall establish controls to ensure that

a. Reproduction is kept to a minimum consistent with mission requirements;

b. Classified material is not reproduced on equipment that poses unacceptable risks;

c. Personnel doing the reproduction are aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take;

d. Reproduced material is clearly identified as classified at the applicable level;

e. Reproduced material is placed under the same accountability and control requirements as apply to the original material; and

f. Waste products generated during reproduction are properly protected and disposed of.

Section 6

Foreign Government Information

6-600 **General**

NATO classified information shall be controlled and safeguarded in compliance with USSAN

Instruction 1-69. Other foreign government information shall be controlled and safeguarded in the manner described in this Chapter for U.S. classified information, except as described below. The control and safeguarding requirements for foreign government information may be modified as required

or permitted by a treaty or international agreement, or, for other obligations that do not have the legal status of a treaty or international agreement (e.g., a contract), by the responsible national security authority of the originating government.

6-601 Foreign Government **Top Secret, Secret and Confidential Information**

a. Top Secret

Records shall be maintained of the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction shall be witnessed. Records shall be maintained for five years.

b. Secret

Records shall be maintained of the receipt, distribution, external dispatch and destruction of material containing foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements. reproduction shall be recorded. Records shall be maintained for three years.

c. Confidential

Records shall be maintained for the receipt and external dispatch of Confidential foreign government information. Other records need not be maintained for foreign government Confidential information unless required by the originating government. Records shall be maintained **for two** years.

6-602 Foreign Government **Restricted Information and Information Provided in Confidence**

In order to ensure the protection of other foreign government information provided in confidence (e.g.,

foreign government “Restricted,” or foreign government unclassified information provided in confidence), such information must be classified under **E.O. 12958**. The receiving DoD Component shall provide a degree of protection to the foreign government information at least equivalent to that required by the foreign government or international organization that provided the information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the information shall be marked as described in Section 7 of Chapter 5 of this Regulation and the following requirements shall be met:

a. The information shall be provided only to those individuals who have an established **need-to-know**, and where access is required by official duties.

b. Individuals given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.

c. Documents shall be stored so as to prevent unauthorized access (e.g., a locked desk or cabinet or a locked room to which access is controlled).

6-603 **Third-Country Transfers**

The release or disclosure of foreign government information to any third-country requires the prior written consent of the originating government.

6-604 **Storage**

To the extent practical, foreign government information should be stored separately from other information to facilitate its control. To avoid additional costs, separate storage may be accomplished by methods such as using separate drawers in the same container as other information or, ‘for small amounts, the use of separate file folders in the same drawer.

Section 7

Disposition and Destruction of Classified Material

6-700 **Policy**

a. Classified documents and other material shall be retained within DoD organizations only if they are

required for effective and efficient operation of the organization or if their retention is required by law or regulation. Documents that are no longer required for operational purposes shall be disposed of in accordance with the provisions of the Federal Records Act (44 U.S.C. Chapters 21, 31 and 33) and

appropriate implementing directives and records schedules. Material that has been identified for destruction shall continue to be protected, as appropriate, for its classification until it is actually destroyed. Destruction of classified documents and material shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

b. Heads of the DoD Components shall ensure that management of retention of classified material is included in oversight and evaluation of program effectiveness. Each activity with classified holdings should establish at least one day each year when specific attention and effort is focused on disposition of unneeded classified material (“clean-out day”).

6-701 Methods and Standards

a. Classified information identified for destruction shall be destroyed completely to preclude

recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by the Head of the DoD Component or their designee. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing.

b. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of **classified** electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

Section 8

Alternative or Compensatory Control Measures

6-800 General

a. This Chapter prescribes the minimum requirements that will normally be applied for the safeguarding of classified information. Senior Agency Officials may, through issuance of appropriate Component guidelines and, consistent with other provisions of this paragraph and subsection 6-801, below, approve the use of alternative or compensatory security controls to ensure that the protection afforded classified information is sufficient to reasonably deter and detect actual or possible compromise. Approval to use alternative or compensatory control measures shall be documented, to include identification of the actual controls employed, and furnished upon request to other agencies with whom classified information or secure facilities are shared. A copy of this documentation must also be provided to the ASD(C3I) or USD(P), as appropriate, for reporting to the Director, Information Security Oversight Office, consistent with paragraph 1-401 .a. of Chapter 1 of this Regulation.

b. Alternative or compensatory security control measures shall be employed only after consideration of risk management factors such as criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability

to exploitation; and countermeasures benefits versus cost.

c. Authority to use any of the following security controls that would extend program-wide and that are program-specific **shall** require the approval of a Component official with original classification authority. The following security controls may **be** applied to another DoD Component or another Executive Branch agency, only with the written agreement of that Component or agency. Moreover, the Component instituting use of any of the following controls shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for use. (The provisions of this subparagraph do not apply to the Single Integrated Operational Plan (SIOP).)

(I) Maintenance of lists or rosters of personnel to whom the classified information has been or may be provided.

(2) Using an unclassified nickname to identify classified information requiring the alternative or compensatory protection. (NOTE: Codewords shall not be used for this purpose. Other special terminology or special markings shall not be used except as prescribed for the handling of message traffic, or as authorized by this Regulation)

(3) Requiring that classified information be placed *in **sealed** envelopes marked **only** with the* nickname and stored in a manner to avoid commingling with other classified files.

(4) Requiring unique DoD Component oversight or inspection procedures.

d. Alternative or compensatory security controls may be applied to contractors only when specifically identified in the DD Form 254, "Department of Defense Contract Security Classification Specification."

e. Alternative or compensatory security controls shall not be applied to Restricted Data.

f. Requests to use alternative or compensatory security controls for the safeguarding of NATO or foreign government information shall be submitted through channels to the Deputy to the Under Secretary of Defense (Policy) for Policy Support.

g. Alternative or compensatory security controls shall not preclude, nor unnecessarily impede, Congressional, Office of the Secretary of Defense, or other appropriate oversight of program or activity functions or operations

6-801 Special Access Controls

The **following** security control measures **shall** be used only in those instances where a program has been approved in accordance with Chapter 8 of this Regulation as a Special Access Program:

a. Personnel security investigative or adjudicative requirements more stringent than those normally required for a comparable level of classified information;

b. Specialized non-disclosure agreements or briefing *statements*;

c. Use of any special terminology; other than a nickname issued in accordance with established JCS procedures, or as prescribed for the handling of message traffic; or special markings, other than those authorized by this Regulation; to identify or control the dissemination of the information that has been determined to require enhanced security controls.

d. Exclusion of a classified contract from inspection by the Defense Investigative Service (use of a carve-out); or

e. A centralized billet system to control the *number of personnel authorized access.*

CHAPTER 7

TRANSMISSION AND TRANSPORTATION

Section 1

Methods of Transmission or Transportation

7-100 Policy

a. Heads of the DoD Components shall establish procedures for transmission and transportation of classified information and information-bearing material that minimize risk of compromise while permitting use of the most cost-effective transmission or transportation means.

b. **COMSEC** information shall be transmitted and transported in accordance with National Telecommunications and Information Systems Security Instruction 4001.

c. NATO classified information shall be transmitted in compliance with USSAN Instruction 1-69.

d. Except under rules established by the **Secretary** of Defense, or as provided by Section 102 of the National Security Act, classified information originating in a department or agency other than the Department of Defense shall not be disseminated outside the Department of Defense without the consent of the originating department or agency.

7-101 Top Secret Information

Top Secret information shall be transmitted only by:

a. Direct contact between appropriately cleared persons.

b. A cryptographic system authorized by the Director, NSA, or a protected distribution system designed and installed to meet the requirements of National Communications Security Instruction 4009. This applies to voice, data, message, and facsimile transmissions.

c. The Defense Courier Service (DCS) if material qualifies under the provisions of DoD Regulation 5200.33-R. The DCS may use a specialized shipping container as a substitute for a DCS courier on direct flights provided that the shipping container is of **sufficient** construction to provide evidence of forced entry, secured with a high security padlock and equipped with an electronic seal that would provide evidence of surreptitious entry, A DCS courier must

escort the specialized shipping container to and from the aircraft and oversee its loading and unloading. This authorization also requires that the DCS develop procedures that address the protection of specialized shipping containers in the event a flight is diverted for any reason.

d. Authorized DoD Component courier services;

e. The Department of State Diplomatic Courier Service;

f. Cleared U.S. military personnel and Government civilian employees specifically designated to carry the information who are traveling on a conveyance owned, controlled, or chartered by the U.S. Government or DoD contractors traveling by surface transportation;

g. Cleared U.S. Military personnel and Government civilian employees specifically designated to carry the information who are traveling on scheduled commercial passenger aircraft within and between the United States, its Territories, and Canada.

h. Cleared U.S. Military personnel and government civilian employees specifically designated to carry the information who are traveling on scheduled commercial passenger aircraft on flights outside the United States, its territories, and Canada.

i. Cleared DoD contractor employees **within** and between the United States and its Territories provided that the transmission has been authorized in writing by the appropriate Cognizant Security Agency (CSA) or a designated representative.

7-102 Secret Information

Secret information may be transmitted by:

a. Any of the means approved for the transmission of Top Secret information;

b. Appropriately cleared contractor employees provided that the transmission meets the requirements specified in DoD 5220.22-R and DoD 5220.22-M.

c. On an exception basis, when applicable postal regulations (39. C. F. R.) are met, Agency Heads may,

when an urgent requirement exists for overnight delivery to a DoD Component within the United States and its Territories, authorize the use of the current holder of the General Services Administration contract for overnight delivery of information for the Executive Branch. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract **shall** require cooperation with government inquiries in the event of a loss, theft, or possible compromise. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the **correct** mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information **shall** not be transmitted in this manner.

d. U.S. Postal Service registered mail within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico;

e. U.S. Postal Service Express Mail within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico. The “Waiver of Signature and Indemnity” block on the U.S. Postal Service Express Mail Label 11-B may not be executed under any circumstances. The use of external (street side) Express Mail collection boxes is prohibited.

f. U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the United States and its Territories, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection;

g. U.S. Postal Service and Canadian registered mail with registered mail receipt between U.S. Government and Canadian Government installations in the United States and Canada;

h. Carriers cleared under the National Industrial Security Program who provide a Protective Security Service. This method is authorized only within the Continental United States (CONUS) when other methods are impractical, except that this method is also authorized between U.S. and Canadian government approved locations documented in a transportation plan approved by U.S. and Canadian government security authorities.

i. Government and Government contract vehicles

including aircraft, ships of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized secure, safe-like container.

j. In exceptional circumstances, with the written approval of the recipient government security authorities, classified material up to an including Secret may be transmitted outside of the United States and its Territories in the hold of a cleared U.S. registered air carrier (Civilian Reserve Air Fleet participant) without an appropriately cleared escort. The shipment must be sent between two specified points with no intermediate stops. The carrier must agree in advance to permit cleared and specifically authorized persons to observe placement and removal of the classified shipment from the air carrier. The shipment must be placed in a compartment that is not accessible to any unauthorized person or in the same type of specialized shipping as is prescribed in subparagraph c. above, for use by the DCS.

7-103 **Confidential Information**

Confidential information may be transmitted by:

a. Means approved for the transmission of Secret information.

b. U.S. Postal Service Registered Mail for:

(1) Material to and from FPO or APO addressees located outside the United States and its Territories.

(2) Material when the originator is uncertain that the addressee’s location is within U.S. boundaries.

c. U.S. Postal Service certified mail (or registered mail, if required above) for material addressed to DoD contractors or non-DoD agencies.

d. U.S. Postal Service first class mail between DoD Component locations anywhere in the United States and its Territories. The outer envelope or wrapper shall be endorsed:

“POSTMASTER: Do Not Forward.”

e. Within CONUS, commercial carriers that provide a Constant Surveillance Service (CSS).

f. In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters must sign a receipt for the material and agree to:

(1) Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded; and

(2). Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

g. Alternative or additional methods of transmission approved by the head of the DoD Component.

7-104 Transmission of Classified Material to Foreign Governments

a. Policy. Classified information and material that has been approved for release to a foreign government in accordance with DoD Directive 5230.11 shall be transmitted by means that ensure proper transfer between representatives of each government. All

international transfers of classified material shall take place through government-to-government channels. The provisions of Appendix H shall be followed.

b. Control and Accountability. Control and accountability of classified material must be maintained until the material is officially transferred to the intended recipient government through its Designated Government Representative.

c. In urgent situations, appropriately cleared employees may be authorized to handcarry classified material in accordance with Section 3 of this Chapter, below, and Appendix H.

d. Each DoD agency executing an international agreement or contract that will lead to the international transfer of classified material will notify the DoD agency responsible for approving the transfer arrangements at the earliest possible point in international deliberations.

7-105 Shipment of Freight

Procedures established for shipment of bulk classified material as freight shall include provisions for shipment in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and actions to be taken in case of non-delivery or unexpected delay in delivery.

Section 2

Preparation of Material for Transmission

7-200 Envelopes or Containers

a. When classified information is transmitted, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering. The following exceptions apply:

(1) If the classified material is an internal component of a **packageable** item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

(2) If the classified material is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information.

(3). If the classified material is an item or equipment that is not reasonably **packageable** and the shell or body is classified, it shall be concealed with an opaque covering that will hide all classified features.

(4) Specialized shipping containers, including closed cargo transporters, may be considered the outer wrapping or cover when used.

(5) When classified material is hand-carried outside an activity, a locked briefcase may serve as the outer wrapper. In such cases, the addressing requirements of paragraph 7-201 a., below, do not apply.

(6) NATO Restricted material need not be double-wrapped when transmitted within the United States. The marking "NATO Restricted" shall not appear on the wrapper.

b. Classified material shall be prepared for shipment, packaged, and sealed in ways that minimize risk

of accidental exposure or undetected deliberate compromise. Documents should be packaged so that classified text is not in direct contact with the inner envelope or container.

7-201 Addressing

a. The outer envelope or container for classified material shall be addressed to an official government activity or to a DoD contractor with a facility clearance and appropriate storage capability and **shall** show the complete return address of the sender. The outer **envelope** shall not be addressed to an individual. Office codes or phrases such as "Attention: Research Department" may be used.

b. The inner envelope or container shall show the address of the receiving activity, the address of the sender, the highest classification of the contents (including, where appropriate, any special markings such as "Restricted Data" or "NATO,") and any applicable special instructions. The inner envelope may have an "attention line" with a person's name.

c. The outer envelope or single container shall not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

d. Classified information intended only for U.S. elements of international staffs or other organizations must be addressed specifically to those elements.

Section 3

Escort or Hand-Carrying of Classified Material

7-300 General Provisiona

a. Appropriately cleared personnel may be authorized to escort or **handcarry** classified material between locations when other means of transmission or transportation cannot be used. Component heads shall establish procedures to ensure that **handcarrying** of classified material is minimized and does not pose unacceptable risk to the information. Handcarrying may be authorized only when:

(1) The information is not available at the destination and is required by operational necessity or a contractual requirement;

(2) The information cannot be sent via a secure facsimile transmission or by other secure means;

(3) The **handcarry** has been authorized by the appropriate official as required by the Component head;

(4) **The** handcarry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the information will remain in the custody and physical control of the U.S. escort at all times.

(5) Arrangements have been made for secure storage at a U.S. Government or cleared U.S. contractor facility.

b. Couriers must be informed of and acknowledge their security responsibilities. The latter requirement may be satisfied by a briefing or by requiring the

courier to read written instructions that contain the information listed below, as a minimum:

(1) The courier is liable and responsible for the material being escorted;

(2) The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies or cleared U.S. contractor facilities must be used. Classified material **shall** not be stored in hotel safes.

(3) The material shall not be opened en route except in the circumstances described in subparagraph 7-300. b.(8), **below**.

(4) The classified material is not to be discussed or disclosed in any public place.

(5) The courier shall not deviate from the authorized travel schedule.

(6). In cases of emergency, the courier must take measures to protect the classified material.

(7) The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents, etc.) are complete, valid, and current.

(8) There is no assurance of immunity from search by the customs, police, **and/or** immigration officials of various countries whose border the courier may cross; therefore, should such officials inquire into the contents of the consignment, the courier shall

present the courier orders and ask to speak to the senior customs, police **and/or** immigration official; this action should normally suffice to pass the material through unopened. However, if the senior **official** demands to **see** the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public.

(a) **Precautions** should be taken to show **officials** only as much of the contents as will satisfy them that the package does not contain any other item. The courier should ask the official to repack the material or assist in repacking it immediately upon completion of the examination.

(b) The senior customs, police and/or immigration **official** should be requested to provide evidence of the opening and inspection of the package by sealing and signing it when closed and confirming the shipping documents (if any) or courier certificate that the package has been opened. Both the addressee and the dispatching security officer shall be informed in writing of the opening of the material.

(c) Classified material to be carried by a courier shall be inventoried; a copy of the inventory shall be retained by the courier's security office and a copy shall be carried by the courier.

(d) Upon return, the courier must return all classified material in a sealed package or produce a receipt signed by the security officer of the addressee organization for any material that is not returned.

(e) For guidance on **handcarrying** NATO classified material, refer to USSAN 1-69.

c. In the event that the handcarry of classified information will also involve the disclosure of classified information to foreign nationals, the DoD Component official responsible for approving the handcarry is also responsible for ensuring that disclosure authorization has been obtained in accordance with DoD Directive 5230.11.

7-301 Documentation

a. Responsible officials **shall** provide a written statement to **all** individuals escorting or carrying classified material authorizing such transmission. This authorization statement may be included in official travel orders except for travel aboard commercial aircraft in which case subsection 7-302, below, applies.

b. The DD Form 2501, "Courier Authorization," may be used to identify appropriately cleared DoD military and civilian personnel who have been

approved to **handcarry** classified material in accordance with the following, except that in the case of travel aboard commercial aircraft the provisions of paragraph 7-302, below, apply:

(1) The individual has a recurrent need to **handcarry** classified information;

(2) The form is signed by an appropriate official in the individual's servicing security office;

(3) Stocks of the form are controlled to preclude unauthorized use.

(4) The form is issued for no more than one year at a time. The requirement for authorization to handcarry shall be **reevaluated** and/or **revalidated** on at least an annual basis, and a new form issued, if appropriate.

(5) The use of the **DD** Form 2501 for **identification/verification** of authorization to handcarry Sensitive **Compartmented** Information or special access program information shall be in accordance with policies and procedures established by the official having security responsibility for such information or programs.

7-302 Hand-carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft

a. Advance coordination should be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this Regulation and Federal Aviation Administration (FAA) guidance, to facilitate the courier's processing through airline ticketing, screening and boarding procedures. **Local** FAA field **offices** can often be of assistance. During this coordination, specific advice should be sought regarding the nature of documentation that will be required. Generally, the following has been found to meet requirements:

(1) The individual designated as courier shall be in possession of a DoD or contractor-issued identification card that includes a photograph, descriptive data, and signature of the individual. (If the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization.)

(2) The courier shall have the original of the authorization letter. A reproduced copy is not acceptable. The traveler shall have sufficient authenticated copies to provide a copy to each airline

involved. The letter shall be prepared on letterhead stationary of the agency authorizing the carrying of classified material and shall:

(a) Give the full name of the individual and his or her employing agency or company;

(b) Describe the type of identification the individual will present (for example, Naval Research Laboratory Identification Card NO. 1234; ABC Corporation Identification Card No. 1234);

(c) Describe the material being carried (for example three sealed packages, 9" X 8" X 24", addressee and addressor);

(d) Identify the point of departure, destination, and known transfer points;

(e) Carry a date of issue and an expiration date;

(f) Carry the name, title and signature of the official issuing the letter. Each package or carton to be exempt shall be signed on its face by the **official** who signed the letter; and

(g) Carry the name of the person designated to confirm the letter of authorization, and that person's **official** U.S. Government telephone number.

b. The traveler should process through the airline ticketing and boarding procedure the same as other passengers. The package or the carry-on luggage containing it should be routinely offered for inspection for weapons.

Chapter 8

SPECIAL ACCESS PROGRAMS

8-100 Policy

It is the policy of the Department of Defense to use the security classification categories and the applicable sections of **E.O. 12958** and its implementing 1S00 Directives to limit access to classified information on a “need-to-know” basis only to those personnel who have been determined to meet requisite personnel security requirements. Further, it is DoD policy to rigorously apply the need-to-know principle in the normal course of controlling collateral classified information so that Special Access Program (SAP) controls will be used only when exceptional security measures are required based on threat and/or vulnerability (e.g. sensitivity or value of the information) associated with the SAP. Need-to-know principles shall also be applied within SAPS. In this **context**, SAPS maybe created or continued only on a specific finding that:

- a. The vulnerability of, or threat to, the specific information to be protected is exceptional;
- b. Normal criteria for determining access to the assigned level of classification are not sufficient to protect the information from unauthorized disclosure;
- c. Careful consideration is given to: assessing the vulnerability, the sensitivity of the information to be protected, and the adequacy of needed safeguarding requirements; and/or
- d. The establishment of the SAP is required by statute.

8-101 SAP Procedures

Unless exempted by the Secretary of Defense or Deputy Secretary of Defense, the DoD SAP Oversight Committee, (**SAPOC**), management structure and its working level Senior Review Group (**SRG**) shall be the forum for addressing the approval and disapproval for all DoD SAPS. In brief, the DoD utilizes a SAP Coordination **Office (SAPCO)**, to support the **SAPOC**. The SAPOC is a matrix management organization that is made up of three **OSD-level** SAP Central Offices. The required approval documents shall be processed through the appropriate Unified Commands or respective component to the appropriate **OSD-level** SAP Central **Office** (i.e., Acquisition SAPS to Director, Special Programs, OUSD (**A&T**)); Operations and Support SAPS, Director, Special Programs, **ODTUSD(P)PS**,

OUSD(P); and Intelligence SAPS, Director, Special Programs, OASD (**C3I**). The **OSD-level** SAP Central **Office** will “sponsor” the program for SAP approval and as apart of the SAPCO **control** it as it is **processed** through the SRG and SAPOC management structures to the Deputy Secretary of Defense, Chairman, SAPOC. In addition, the **OSD-level** SAP Central **Offices** must be advised of **all non-DoD** SAPS that have DoD participation (e.g., DoD personnel performing any program **functions**). SAPS that are NOT DoD SAPS, but which have active DoD support must be reported to one of the three cognizant **OSD-level** Central Offices. Specifically:

- a. SAPS involving NATO classified information are based on international treaty requirements. DoD involvement with these SAPS must be reported to the Director, Special Programs, **ODTUSD(P)PS**, **OUSD(P)**.
- b. The policies and procedures for access to and dissemination of Restricted Data, (**RD**) and Critical Nuclear Weapon Design Information, (**CNWDI**) are contained in DoD Directive 5210.2. Any SAPS associated with RD and **CNWDI** must be reported to the Director, Special Programs, **ODTUSD (P)PS**, **OUSD(P)**.
- c. SAPS protecting foreign intelligence information under the cognizance of the Director of Central Intelligence (**DCI**) must be reported appropriately to either the Director, Special Programs, **ODTUSD(P)PS**, **OUSD(P)**, or the Director, Special Programs, **OASD(C3I)**, or to both. The National Security Act of 1947 and **E.O. 12958** authorize the **DCI** to create SAPS pertaining to intelligence activities in accordance with Director of Central Intelligence Directive 3/29. The DCI is not authorized to create SAPS for military operational, strategic and tactical programs that are under the cognizance of the DoD.
- d. When a DoD Component is involved with a SAP(s) or SAPS that involves one or more other DoD Component(s) or a **non-DoD** activity, DoD Components shall:

- (1) Formalize or document the relationship in a written agreement (e.g., Memorandum of Agreement or Memorandum of Understanding) that specifies who has primary sponsorship of the program, and responsibility for obtaining SAP

approval.

(2) Provide **to the appropriate OSD-level** SAP Central **Office** notice that agreements have been executed with other DoD or non-DoD activities and make the details of the association available during oversight reviews as prescribed in DoD Directive 0-5205.7 and this Regulation.

e. Activities that do not involve acquisition or intelligence funds, and that protect purely military operations or the support thereof, are not reported or considered to be a DoD SAP per se. Rather, the activities within these programs are reported to the leadership and membership of Congress in the context of report of military operations as determined by the President and the Secretary of Defense.

f. SAPS involving participation by foreign governments shall be in compliance with DoD Directive 5230.11.

8-102 **Control and Administration**

a. SAPS shall be controlled and managed in accordance with DoD Directive 0-5205.7. The processes of the SAPOC, the SRG, the **SAPCO**, and the Special Access Program Policy Forum facilitate standardized and uniform security procedures and requirements. Specific responsibilities of the SAPOC, SRG, SAPCO, and SAP Policy Forum are defined in DoD Directive 0-5205.7.

b. The three **OSD-level** SAP Central Offices (Acquisition, Intelligence, and Operations and Support) have primary responsibility for (and authority over): (1) the types of activities conducted in the SAPS under their areas of cognizance; (2) endorsing or negotiating a change of the assigned category of a SAP, (3) collating, coordinating, and forwarding the SAPS annual reports; (4) conducting oversight reviews, as required; (5) reviewing and endorsing terminating or **transitioning** plans; and (6) ensuring SAPS do not duplicate or overlap other programs under its purview.

c. Each DoD Component shall establish a Component-level SAP Central Office to coordinate SAP requests for approval and otherwise “mirror” the activities of the three **OSD-level** SAP Central Offices. In addition to the specific responsibilities set forth in DoD Directive 0-5205.7, Component-level SAP Central **Offices** shall maintain records of **all** SAPS and Prospective SAPS, (P-SAPS), under their cognizance to include approval documentation and, if appropriate, **revalidation** documentation. Records shall be retained for the life of the SAP and for 12

months after termination of the program.

d. In accordance with DoD Directive 5010.38 and **Office** of Management and Budget Circular A-123, the DoD Management Control Program (**MCP**) will be implemented within all SAPS. To ensure adequate implementation, DoD Components are required to have MCP coordinators within special access channels to:

(1) Provide guidance, training, and oversight on the MCP to SAP managers;

(2) Serve as the central point to which all SAP deficiencies (of a classified nature) that are identified through the MCP are reported; and

(3) Establish formal follow-up systems to ensure that SAP managers schedule corrective actions for all reported deficiencies to include monitoring deficiencies until resolved. Each Component will prepare an annex on SAPs to their annual statements of assurance to the Secretary of Defense or assert in their annual statement that no material weaknesses were reported within their SAPS. In either case, statements will be classified, if required, and will be sanitized from **all** special access program specific information. Reports will be reviewed by Component-level SAP Central Offices prior to forwarding outside SAP channels.

e. Unless specifically exempted by the SAPCO, SAP contract administration services shall be delegated to the Defense Contract Management Command’s (**DCMC**) dedicated cadre of personnel. Also, the DCMC shall utilize the dedicated cadre of personnel of the Defense Contract Audit Agency for audit services, unless specifically exempted.

8-103 **Establishment of DoD SAPS**

a. In accordance with **E.O.** 12958, within the Department of Defense, only the Secretary of Defense or **Deputy** Secretary of Defense may create a SAP. The DoD Components proposing the establishment of SAPS shall evaluate and process proposals in accordance with the procedures in this Regulation, DoD Directive 0-5205.7 and other implementing directives. DoD Components are responsible for ensuring that Unified Combatant Commands are appropriately briefed and consulted during the development process. A SAP may not be initiated until the defense committees of Congress are notified of the program and a period of 30 days elapses after such notification is received.

b. The military Departments SAP Central Offices

or **OSD-level** SAP Central **Offices** may authorize a Prospective SAP (P-SAP). Upon authorization, enhanced security measures (i.e., SAP controls) may be applied to a P-SAP for up to 6 months. The program must be terminated if not submitted to SAPOC process after 6 months or formally extended by the Director, **SAPCO**. Except for minor administrative security operations and maintenance (“**O&M**”) funds needed to maintain security, no direct funding may be expended on any P-SAP without the required notifications to Congress. Transitional funds for associated efforts in some instances are authorized where direct funding is not applicable. In all cases, the Director or Deputy Director SAPCO must be notified of the establishment or termination of **P-SAPS** through the appropriate **OSD-level** SAP Central **office**.

c. Before initiating a SAP, notifying Congress, or expending funds on a SAP, the DoD Components shall forward a request for approval of the SAP and relevant funding documentation to the Deputy Secretary of Defense through the appropriate **OSD-level** SAP Central Office for processing through **SAPOC** management structure. The Director, Special Programs, **ODTUSD(P)PS**, **OUSD(P)** shall review the security requirements on behalf of the SAPOC.

d. The request package shall include the following:

(1) Identification of the responsible office or DoD Component, including office designation and symbols. Identification of the Component-level SAP Central Office **official** who is the point of contact for the SAP (full name, position or title, mailing address, and telephone number).

(2) The unclassified nickname(s) and, if used, the classified code word(s) for the SAP and its **subelements** or subcompartments. NOTE: All DoD SAPs shall have an unclassified nickname assigned and utilized.

(3) The designation of the SAP’s category as an Acquisition, Intelligence, or Operations and Support SAP and whether the SAP is unacknowledged or acknowledged. The type of funding being used and the associated recommendation of the sponsoring DoD Component and subsequent Deputy Secretary of Defense approval determines the category. The DoD SRG may make appropriate recommendations for a change in a SAP category as a part of the annual review process.

(4) The relationship, if any, to other DoD

and/or non-DoD SAPS, to include the identification of existing agreements, memorandums of understanding, or similar arrangements that pertain to the proposed DoD SAP.

(5) Justification for establishing the Program as a SAP, including the reasons why normal management and safeguarding procedures for classified information are not **sufficient**, a description of the threat that can exploit identified **vulnerabilities**, and how the additional special security procedures will compensate for or mitigate those **vulnerabilities**.

(6) Budgetary information in the format contained in Appendix I.

(7) The total estimated number of persons who will require access to the SAP during the first year. Separate the total into the following categories: sponsoring DoD **Component**; other DoD Components and activities; other Government Agencies; contractors; and elsewhere in the private sector.

(8) A program security classification guide, a program security policy and procedures plan, and an operational policy. The security policy and procedures plan shall include personnel security, physical security, automated information systems security, etc., and proposed counterintelligence and operations security requirements and support. These documents should embody any “risk management” concepts that are applied.

(9) If contractors are a part of the program, a statement that a **DD Form 254, Contract Security Classification Specification**, has been issued to contractors participating in the program. The statement will include identification of which elements **and/or** overprinted elements of DoD 5220.22-M-Sup. 1, **National Industrial Security Program, Operating Manual Supplement, (NISPOMSUP)** apply to the SAP.

(10) If applicable, a request and justification for waiver to any specific criteria specified by this Regulation and, if applicable, the DoD 5220.22-M-Sup. 1.

(11) If applicable, a justification for those functions that **will** be performed by the SAP that are normally performed by centralized organizations or specialized cadres of personnel who are dedicated to performing SAP-related functions within those organizations (e.g. contract administration services, contract payment, travel reimbursement). Specifically, if contracting is part of the SAP, a

request must be made to relieve or “carve-out” the Defense Investigative Service (**DIS**), see Carve-Out Contracts, paragraph **8-103e.**, below. In some instances where the normal organizations are not used, it must be fully explained how the required tasks, security and other unique tasks, will be performed for the SAP.

(12) If applicable, a request and justification to waive the SAP reporting requirements specified by Section 119(e), title 10, United States Code.

(13) Identification of those members of Congress and Congressional staffs who have knowledge of the SAP in its proposed configuration or in some earlier form.

(14) Proposed Congressional notification letters to the chairperson and ranking minority member of: the Committee on National Security, House of Representatives, the Committee on Armed Services, United States Senate, the Subcommittee on Defense, Committee on Appropriations, House of Representatives, and the Subcommittee on Defense, Committee on Appropriations, United States Senate. See format in Appendix I.

(15) The endorsement by the head of the sponsoring DoD Component, and a request for approval by the Deputy Secretary of Defense forwarded through the appropriate **OSD-level SAP Central Office** having program cognizance, to the Director, SAPCO.

(16) The date that the program is scheduled to be established and any associated constraining time frames.

e. Carve-Out Contracts

(1) The use of contracts that relieve DoD organizations of their established contract related responsibilities must be fully explained and justified. If the SAP will perform the functions of review and/or inspection, the responsibilities of the Cognizant Security Office(s), or investigative functions, a request must be made to relieve DIS from their responsibilities under the National Industrial Security Program, and the practice must be identified as a “carve-out”. Carve-outs are prohibited unless:

(a) The contract in question supports a SAP that has been approved by the **SAPOC**.

(b) Mere knowledge of the existence of a particular contract or its association with the SAP is classified and designated as SAP protected informa-

tion; and

(c) The carve-out status for the SAP on its contract was approved as a part of the DoD SAPOC process.

(2) The DD Form 254, classified if necessary, shall be used to document a carve-out contract. The DD Form 254 shall identify specific areas, or locations within a contractor’s facility that define the extent of the carve-out, (e.g., a safe, a room, or a particular building). It will also identify the CSO and CSA. The Component-level SAP Central Office shall provide a copy of each DD Form 254 to the appropriate DIS cognizant security **office** and, if applicable, to the Director, Defense Contract Audit Agency (DCAA). In exceptional instances the **OSD-level SAP Central Office** may, with concurrence of the Director, Special Programs, **ODTUSD(P)**, **OUSD(P)** convey appropriate written notification defining the extent of the carve-out directly to the Director, DIS, and if applicable to the Director, DCAA.

(3) Approved carve-out contracts shall be afforded the support from the sponsoring **Component-level SAP Central Office** for the protection of the classified information involved. The support **shall** be provided through a system of controls that includes, but is not limited to, the following elements:

(a) Designate a central office of record and an official designated to be the single point of contact for SAP security planning, control, and administration. These security plans shall be submitted to the Director, Special Programs, **ODTUSD(P)**, **OUSD(P)** for review and endorsement as a part of the SAPOC approval process.

(b) A Written Security Plan. The plan will include, if applicable, how security will be accomplished for contractors. An overprinted DoD 5220.22-M-Sup. 1 will be provided if contracts are a part of the SAP. Oral changes or deviations from the written plan are prohibited except in critical situations. These changes will be documented as soon as practicable after the fact.

(c) Security Review Procedures. The procedures will ensure that fully qualified government professional security personnel of the sponsoring DoD Component perform security reviews at each contractor’s facility with the frequency, generally, prescribed by DoD 5220.22-M-Sup. 1. NOTE: Reviews for cause or supporting visits may be as frequently as warranted by “risk management” principles.

(d) Specialized procedures to be followed for developing and implementing contracts for unacknowledged SAPS.

f. Nicknames and Code words

(1) Each DoD SAP shall be assigned an unclassified nickname. Classified code words may also be assigned to SAPS but are optional. Military Departments and DoD Components shall develop a system to assign and administer nicknames and code words for SAPS for their Departments. The DoD Components other than the Military Departments may request nicknames and code words for SAPS from the appropriate **OSD-level SAP Central Office**, (See Chairman of the Joint Chiefs of Staff Manual **CJCSM 3150.29** for more information.)

(2) **Non-DoD** originated nicknames and code words used by DoD Components participating in **non-DoD** SAPS shall be registered with the appropriate **OSD-level SAP Central Office** and the JCS central registry to prevent confusion with DoD-originated words. (NOTE: Some **non-DoD** Executive Branch organizations do not observe the same two word **and/or** nickname and one word **and/or** code word policy as does the DoD.)

(3) Within the Department of Defense, a nickname is a combination of two separate unclassified words. Do not use combination of words including “project,” “exercise,” or “operation” or words that may be used correctly either as a single word or as two words, such as moon-light. Do not use exotic words, trite expressions, or well-known commercial trademarks. A nickname should not:

(a) Express a bias inconsistent with traditional American ideals or foreign policy.

(b) Convey connotations offensive to good taste or derogatory to a particular group, sect, or creed, or

(c) Convey connotations offensive to our allies or other nations, or

(d) Be discussed on an unclassified communication net unless **all** aspects including organizational associations are completely unclassified. (NOTE: The use of STU III while discussing or mentioning nicknames is very strongly encouraged.)

(4) Within the Department of Defense, a code word is a single word assigned a classified meaning by appropriate authority. It is classified as

CONFIDENTIAL or higher. A code word **shall** not be assigned to test, drill, budget identifiers, or exercise activities. The using Component shall assign to a code word a specific meaning classified SECRET or CONFIDENTIAL. Code words shall not be used to cover unclassified meanings. TOP SECRET code words may be issued only with Director, Special Programs, **ODTUSD(P)**, **OUSD(P)** approval or by the DoD component in coordination with the Director, Special Programs, **ODTUSD(P)**, **OUSD(P)**. The assigned meaning need not in all cases be classified as high as the overall classification assigned to the program or operation. Code words shall not suggest the nature of its meaning. It shall not be used repeatedly for similar purposes; that is, if the initial phase is designated “Meaning,” succeeding phases should not be designated “Meaning II” and “Meaning III,” but should have different code words. Each DoD Component **shall** establish policies and procedures for the control and assignment of classified meaning to code words. No code word may be discussed on an unclassified communication net or telephone.

8-104 Reviews of SAPS

a. To facilitate management’s stewardship over SAPS, each DoD SAP shall be reviewed annually by the DoD Component responsible for initiation and sponsorship of the program, in coordination with appropriate Unified Combatant Commands. These reviews shall include annual regularly scheduled audits by security, contract administration, and audit organizations. Written records of these reviews and audits shall be maintained for the lifetime of the SAP and for 12 months following its termination. These records **shall** be available for evaluation during the **OSD-level SAP Central Office** program reviews.

b. As part of the annual reporting and revalidation of **all** DoD SAPS, the DoD Components shall ensure that these programs continue to be reviewed by qualified legal counsel for compliance with applicable laws, executive orders, and regulations.

c. The **OSD-level SAP Central Offices** shall conduct oversight reviews, as required, to determine compliance with DoD Directive 0-5205.7 and this Regulation, to specifically include verification of the conduct of Component-level annual security reviews.

d. The **ODTUSD(P)PS**, **OUSD (P)**, shall conduct appropriate annual oversight reviews of each SAP Central Office and, as deemed necessary, on-site program security reviews at Government and contractor locations.

e. The Inspector General of the Department of Defense shall conduct oversight of DoD SAPS, pursuant to statutory authority.

f. Oversight, review, and SAP support activities **shall** accomplish their functions using small cadres of specially cleared and qualified personnel, **sufficient** in size to address the SAP workload. The cadre's primary responsibility is to support SAPS.

8-105 Annual Reports and Revalidation

a. Section 119 of title 10, United States Code requires that not later than March 1 of each year, the Secretary of Defense shall report all DoD SAPS to Congress. These annual reports also serve as the vehicle for **revalidation** and approval for continuation of all DoD SAPS by the Deputy Secretary of Defense. Any SAP not granted approval to continue shall be terminated.

b. Not later than December 15 of each year, the Component-level SAP Central Office shall submit reports for the Deputy Secretary of Defense on all SAPS under their sponsorship. Since the President's budget may not be available by that date, provide the best estimate as a part of the report with actual budget numbers being provided as soon as they are available.

c. For each SAP sponsored, the DoD Components shall prepare separate reports and "Quad Charts" in the format shown in Appendix I in both MS Word and hard copy. The reports and "Quad Charts" shall be forwarded to the appropriate Component-level SAP Central **Office** for processing. All information elements may not apply to all SAPS; however, as a minimum, each report must include:

(1) Justification for continuation of the Program as a SAP;

(2) If applicable, justification for continuation of the exclusion of the SAP from the review requirements of the National Industrial Security Program (i.e., continuation of carve-out status); and,

(3) If applicable, justification for continuation of status as a Waived SAP under Section 119(e), title 10, United States Code.

d. Components' submissions shall also include a certification that there are no unreported SAPS or SAP-like programs, or an explanation for any programs not included in the report. Any SAP being terminated or unfunded must be clearly identified.

e. The Component-level SAP Central Office shall

aggregate reports by category of SAP (acquisition, intelligence, and operations and support), and shall forward them to the appropriate **OSD-level** SAP Central Office. The **OSD-level** SAP Central Offices shall collate and forward the reports to the Director, SAPCO for Deputy Secretary of Defense action. After action by the Deputy Secretary of Defense, the reports will be returned to the SAPCO.

f. The **SAPCO** notifies Congress of the Deputy Secretary of Defense's decisions **and** then returns the reports to the **OSD-level** SAP Central **Offices** for distribution and action.

g. SAPS that are approved by the Deputy Secretary of Defense as Waived SAPS under Section 119(e), title 10, United States Code, shall be reported on a case-by-case basis to appropriate members of Congress, in accordance with applicable law, with specific direction from the Secretary or Deputy Secretary of Defense.

8-106 Interim Reports

The Component-level SAP Central Office shall immediately notify (through the **OSD-level** SAP Central Office) the Director, SAPCO, when there is a SAP or subcompartment nickname or code word change. Any additions, deletions, or corrections to ~~the~~ annual report should be reported as they occur during the year to include subcompartments. The interim report **shall** contain, at a minimum, the **nickname** affected, effective date of the change, and information that has been changed from the previous report.

8-107 Changes in Classification

a. DoD Components intending to downgrade the classification of a SAP, transition from unacknowledged to acknowledged, remove enhanced controls from a SAP and/or move the program to a collateral security level, declassify a program, or make a public announcement concerning any of these activities, shall prepare letters of notification to the appropriate Congressional Committees in accordance with the format in Appendix I. This requirement also applies to significant **subelements** or subcompartments of SAPS that could potentially be of interest to the Congress (i.e., generally this will necessitate reporting acquisition SAP **subelements** and most major **subelements** of intelligence, and operation and support SAPS, and when sub-compartments are not significant enough to be separately reported, these instances will be coordinated with the appropriate OSD SAP Central Office). This reporting requirement also applies to programmatic information

that is being made public. The DoD Components shall forward these letters through the appropriate Component-level, **OSD-level** SAP Central **Offices**, and the Director, SAPCO, for processing to the Deputy Secretary of Defense. The letter shall contain a description of the proposed change, the reasons for the proposed change, and notice of any public announcement planned to be made about to the proposed change.

b. After approval and signature by the Deputy Secretary of Defense, notification letters shall be returned to the **SAPCO** for delivery to Congress by the DoDC component or the **SAPCO**. No action relative to the change in classification or enhanced security measures (i.e., removal from or change SAP status) of the SAP shall be taken or any announcement made sooner than 14 days after the letters have been delivered to the appropriate committees in Congress, unless authorized pursuant to statute by the Deputy Secretary of Defense.

8-108 **Termination and Transitioning of SAPS**

a. SAPS shall be carefully but promptly terminated or transitioned to collateral security programs when there is no longer a need for the enhanced security protection.

b. DoD sponsoring Components shall prepare SAP termination plans (i.e., a Plan of Action and Milestones, how the “de-sapped” program will comply with the Acquisition System Protection requirements). The plan will outline the security measures that will be followed when terminating or transitioning a SAP. The plan shall identify information that will remain classified and as appropriate, the OPSEC measures designed to protect any sensitive unclassified indicators, or methods associated with the SAP. A time and/or event phased (as deemed most appropriate) Security Classification Guide shall be included in the plan. The plan shall take into consideration continuing collateral security requirements in all functional areas to include the technical aspects, funding, contracting operations, legal, logistics, training, and administrative requirements. The DoD Components shall forward the termination and/or transitioning plan to the appropriate **OSD-level** SAP Central Office for review and endorsement.

c. In all cases, the notification procedures set forth in subsection 8-107 above, shall be followed before actual termination or transition of a SAP is effected.

CHAPTER 9

SECURITY EDUCATION AND TRAINING

Section 1

Policy

9-100 General Policy

Heads of DoD Components shall ensure that personnel of their organization receive such security education and training as may be required to:

- a. Provide necessary knowledge and information to enable quality performance of security functions;
- b. Promote understanding of Information Security Program policies and requirements and their importance to the national security;
- c. Instill and maintain continuing awareness of

security requirements and the intelligence threat; and

- d. Assist in promoting a high degree of motivation to support program goals.

9-101 Methodology

Security education and training may be accomplished through establishment of programs within the Component, use of external resources such as the Department of Defense Security Institute, or a combination of the two.

Section 2

Initial Orientation

9-200 Cleared Personnel

a. All personnel in the organization who are cleared for access to classified information shall be provided an initial orientation to the Information Security Program before being allowed access to classified information. This initial orientation is intended to produce a basic understanding of the nature of classified information and the importance of its protection to the national security, place employees on notice of their responsibility to play a role in the security program, and provide them enough information to ensure proper protection of classified information in their possession. Security educators should consider including:

(1) Roles and Responsibilities

- (a) Who are the senior agency official and agency security personnel and what are their responsibilities?
- (b) What are the responsibilities of agency employees who create or handle classified information?
- (c) Who should be contacted in case of questions or concerns about security matters?

(2) Elements of Classifying and Declassifying Information

- (a) What is classified information and why is it important to protect it.?

- (b) What are the levels of classified information and the damage criteria associated with each level?

- (c) What classification markings are to be used and why is it important that they be properly applied?

- (d) What are the general requirements for declassifying information?

- (e) What are the procedures for challenging the classification status of information?

(3) Elements of Safeguarding

- (a) What are the proper procedures for safeguarding classified information?

- (b) What constitutes a compromise of classified information and what are the penalties associated with compromises?

- (c) What are the general conditions and restrictions for access to classified information?

(d) What should an individual do when he or she believes safeguarding standards have been violated?

(e) What steps should be taken in an emergency evacuation situation?

(f) What are the appropriate policies and procedures for transmission of classified information?

b. Before being granted access to classified information, employees must sign Standard Form 312, "Classified Information Nondisclosure Agreement." Cleared personnel who have signed an earlier nondisclosure agreement, the SF 189, need not sign SF 312, but they may elect to replace their SF 189 with a

signed SF 312. SFS 189 and 312 shall be maintained for 50 years from the date of signature.

9-201 Uncleared Personnel

Members of the organization who are not cleared for access to classified information should be included in the security education program if they will be working in situations where inadvertent access to classified information might occur or will have access to unclassified information that might be of value to intelligence collectors. They should be provided with a brief explanation of the nature and importance of classified information and actions they should take if they discover classified information unsecured, note an apparent security vulnerability, or believe they are contacted by an intelligence collector.

Section 3

Special Requirements

9-300 General

Members of the organization in positions that require performance of specified roles in the Information Security Program shall be provided security education and training sufficient to permit quality performance of those duties. The education and training shall be provided before, concurrent with, or not later than six months following assumption of those positions.

9-301 Original Classifiers

The security education and training provided to original classification authorities shall, as a minimum, address each of the following:

- a. What is the difference between original and derivative classification?
- b. Who can classify information originally?
- c. What are the standards that an original classifier must meet to classify information?
- d. What is the process for determining duration of classification?
- e. What are the prohibitions and limitations on classifying information?
- f. What are the basic markings that must appear on classified information?

g. What are the general standards and procedures for declassification?

h. What are the requirements and standard for creating, maintaining and publishing security classification guides?

9-302 Declassification Authorities Other Than Original Classifiers

The security education and training provided declassification authorities other than original classifiers shall, as a minimum, address each of the following:

- a. What are the standards, methods and procedures for declassifying information under Executive Order 12958 and this Regulation?
- b. What are the standards for creating and using declassification guides?
- c. What is contained in the Component's declassification plan?
- d. What are the Component's responsibilities for the establishment and maintenance of a declassification database?

9-303 Derivative Classifiers, Security Personnel and Others

Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information shall receive training that, as a minimum, addresses the following:

- a. What are the original and derivative classification processes and the standards applicable to each?
- b. What are the proper and complete classification markings to be applied to classified information?
- c. What are the authorities, methods and processes for downgrading and declassifying information?
- d. What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?
- e. What are the requirements for creating and updating classification and declassification guides?
- f. What are the requirements for controlling access to classified information?
- g. What are the procedures for investigating and reporting instances of actual or potential compromise of classified information and the penalties that may be associated with violation of established security policies and procedures?

h. What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

i. What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

j. What are the requirements for oversight of the security classification program, including self-inspections?

9-304 **Others**

Additional security education and training may be required for personnel who::

a. Use automated information systems to store, process, or transmit classified information;

b. Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely;

c. Will be escorting, handcarrying, or serving as a courier for classified material;

d. Are authorized access to classified information requiring special control or safeguarding measures; or

e. Are involved with international programs; or

f. Are involved with acquisition programs subject to DoD Directive 5000.1

Section 4

Continuing Security Education/Refresher Training

9-400 **Continuing Security Education**

Security education should be a continuous, rather than a periodic influence on individual security performance. Periodic briefings, training sessions, and other formal presentations should be supplemented with other information and promotional efforts to ensure maintenance of continuous awareness and performance quality. The use of job performance aids and other substitutes for formal training is encouraged when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a "read-and initial" basis shall not be considered as a

sole means of fulfilling any of the specific requirements of this Chapter.

9-401 Refresher Training

As a minimum, personnel shall receive annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or

concerns identified during Component **self-**

inspections

Section 5

Termination Briefings

9-500 General

The DoD Components shall establish procedures to ensure that cleared employees who leave the organization or whose clearance is terminated receive a **termination** briefing. This briefing shall emphasize their continued responsibility to:

a. Protect **classified** information to which they have had access;

b. Provide instructions for reporting any unauthorized attempt to gain access to such information;

c. Advise the individuals of the prohibition against retaining material when leaving the organization; and

d. Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

Section 6

Program Oversight

9-600 General

Heads of the DoD Components shall ensure that security education programs are appropriately evaluated during self-inspections and other oversight activities. This evaluation shall include assessment of the quality and effectiveness of security education

efforts, as **well** as ensuring appropriate coverage of the target populations. Heads of the Components shall require maintenance of whatever records of programs offered and employee participation they deem **necessary** to permit effective oversight.

CHAPTER 10

ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

10-100 Policy

a. The compromise of classified information can present a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of documents or material that were compromised. In all cases, appropriate action must be taken to **identify the** source and reason for the actual or potential compromise and remedial action to be taken to prevent recurrence.

b. Actual or potential compromises involving cryptologic information shall be handled in accordance with NACSI 4006.

c. Actual or potential compromises involving **SCI** will be handled in accordance with DoD S-5105.21-M-I.

10-101 Reporting

a. Anyone finding classified material out of proper control shall take custody of and safeguard the material, if possible, and immediately notify the appropriate security authorities.

b. Any person who becomes aware of the possible compromise of classified information **shall** immediately report it to the head of his or her local activity or to the activity security manager. If the person believes that the head of the activity or the **security** manager may have been involved in the incident, he or she may report it to the security authorities at the next higher **level** of command or supervision.

c. If classified information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. Report the matter as instructed by the appropriate DoD Component directives, but do not discuss it with anyone without an appropriate security clearance and **need-to-know**. If approached by a representative of the media who wishes to discuss information you believe is classified, neither confirm nor deny the accuracy of or the classification of the information, and report the

situation immediately to the appropriate security and public affairs authorities.

d. Any incident in which deliberate compromise of classified information or involvement of foreign **intelligence** agencies is suspected as well as apparent violations of criminal law **shall** be reported in accordance with DoD Instruction 5240.4. The Principal Director, Information Warfare, Security, and Counterintelligence (**PD(IWSCI)**); **OASD(C3I)**, is the focal point for investigative matters involving the actual or potential compromise of classified information directed to the Department of Defense by other government agencies or that may involve other government agencies.

e. Local security officials will advise their parent command security officials of compromises occurring within their security cognizance and involving personnel assigned to that parent command.

f. If the head of an activity or the activity security manager to whom an incident is initially reported does not have security cognizance over the incident, such official shall ensure that the incident is reported to the appropriate authority. The organization with security cognizance shall ensure that an inquiry/investigation is conducted consistent with this chapter and for taking corrective action as required.

g. All compromises involving computer systems, terminals, or equipment shall be reported through appropriate channels to the Director, Information Assurance, Office of the Deputy Assistant Secretary of Defense (Command, Control and Communications) (**DASD(C3)**).

h. Compromises involving foreign government information shall be reported to the Director of International Security Programs, **OUSD(P)**, who shall notify the foreign government.

i. Compromises involving DoD Special Access Programs, or results of inquiries/investigations that indicate that weaknesses or **vulnerabilities** in established SAP policy and/or procedures contributed to a potential compromise, shall be reported to the Director, Special Programs, **OUSD(P)**.

j. Results of inquiries/investigations into actual or potential compromises that indicate that defects in the procedures and requirements of this Regulation contributed to the incident shall be reported to the PD(IWSCI), OASD(C3I).

10-102 Inquiry/Investigation

a. **Preliminary Inquiry.** When an actual or potential compromise of classified information occurs, the head of the activity or activity security manager having security cognizance shall promptly initiate an inquiry into the incident to determine the following. If information obtained as a result of the preliminary inquiry is sufficient to provide answers to these questions, then such information shall be sufficient to resolve the incident to include institution of administrative sanctions under Section 5, Chapter 1 of this Regulation:

(1) When, where, and how did the incident occur? What persons, situations, or conditions caused or contributed to the incident?

(2) Was classified information compromised?

(3) If a compromise occurred, what specific classified information and/or material was involved?

(4) If classified information is alleged to have been lost, what steps were taken to locate the material?

(5) In cases of compromise of classified information to the public media, the inquiry should determine:

(a) In what specific medial article or program did the classified information appear?

(b) To what extent was the compromised information disseminated?

(c) Was the information properly classified?

(d) Was the information officially released?

(6) If there was no compromise, was there a failure to comply with established security practices and procedures that could lead to compromise if left uncorrected and/or, is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?

b. **Investigation.** If the circumstances of an incident are such that a more detailed investigation is necessary, then an individual will be appointed to

conduct that investigation. This individual must have an appropriate security clearance, have the ability to conduct an effective investigation, and must NOT be someone likely to have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the activity security manager should not be appointed to conduct the investigation. In cases of compromise of classified information to the public media, the investigation should expand upon paragraph 10- 102a.5. above, to include:

(1) Are there any leads to be investigated that might lead to identification of the person responsible for the compromise?

(2) Will further inquiry increase the damage caused by the compromise?

10-103 Results of the Inquiry/Investigation

a. If the conclusion of the inquiry/investigation is that a compromise occurred, the official initiating the inquiry/investigation shall immediately notify the originator of the information or material involved. If the originating activity no longer exists, the activity that inherited the functions of the originating activity shall be notified. If the functions of the originating activity were dispersed to more than one other activity, the inheriting activity (ies) cannot be determined or, the functions have ceased to exist, the senior agency official of the DoD Component of which the originating activity was a part, shall be notified. This notification shall not be delayed pending completion of any additional inquiry/investigation or resolution of other related issues.

b. If the conclusion of the inquiry/investigation is that a compromise occurred and that a weakness or vulnerability in established security practices and/or procedures contributed to the compromise or that the potential exists for a compromise of classified information due to a weakness or vulnerability in established security practices and/or procedures, the appropriate responsible security official shall take prompt action to issue new or revised guidance as necessary to resolve identified deficiencies.

c. If the conclusion of the inquiry/investigation is that a compromise did not occur but that there was potential for compromise of classified information due to a failure of a person or persons to comply with established security practices and/or procedures, the official having security cognizance over such persons or persons shall be responsible for taking action as may be appropriate to resolve the incident.

10-104 Verification, Reevaluation and Damage Assessment

a. When notified of the compromise of classified information or material, the original classification authority for that information or material shall:

(1) Verify the classification and duration of classification initially assigned to the information.

(2) Reevaluate the classification of the information to determine whether the classification should be continued or changed. This review should consider the following possibilities:

(a) The information has lost all or some of its sensitivity since it was initially classified, and should be downgraded or declassified. (In rare cases, it might also be discovered that the information has gained sensitivity, and should be upgraded.)

(b) The information has been so compromised by this incident that attempting to protect it further is unrealistic or inadvisable, and it should be declassified.

(c) The information should continue to be classified at its current level.

(3) Complete a damage assessment in accordance with DoD Instruction 5240.11.

b. While performing the reevaluation and damage assessment, the original classification authority must consider countermeasures that can be taken to minimize or eliminate the damage to the national security resulting from the compromise and then initiate or recommend adoption of such countermeasures. These countermeasures might include changing plans or system design features, revising operating procedures, providing increased protection to related information (through classification or upgrading), etc.

c. The verification, reevaluation and damage assessment process is to be completed as soon as possible following notification of a compromise. However, damage assessment requiring multi-disciplinary or multiple agency review of the adverse effects of the compromise on systems, operations, and/or intelligence, can sometimes be a long-term process.

d. When classified information under the control of more than one DoD Component or other agency is involved, the affected activities are responsible for coordinating their efforts in reevaluation and damage assessment.

10-105 Debriefings in Cases of Unauthorized Access

In cases where a person has had unauthorized access to classified information, it may be advisable to discuss the situation with the individual to enhance the probability that he or she will properly protect it. The activity head shall determine if a debriefing is warranted. This decision must be based on the circumstances of the incident, what is known about the person or people involved, and the nature of the classified information. The following general guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance but no need-to-know, debriefing is usually appropriate only so far as necessary to ensure that the individual is aware that the information to which they had unauthorized access is classified and requires protection.

b. If the unauthorized access was by U.S. Government civilian or military personnel or an employee of a cleared U.S. Government contractor, without the appropriate security clearance, debriefing is usually appropriate. The person should be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if they fail to do so. The debriefing should be designed to ensure that the individual understands what classified information is, why its protection is important, and knows what to do should someone try to obtain the information. In the case of non-DoD personnel and employees of U.S. Government contractors, the appropriate security official in the individual's parent organization, to include the appropriate Facility Security Officer, should be advised of the debriefing.

c. If the person involved is neither member of a U.S. Government organization nor an employee of a cleared contractor, the decision is much more situational. The key question to be decided is whether the debriefing will have any likely positive effect on the person's ability or willingness to protect the information.

d. In any case where the person to be debriefed may be the subject of criminal prosecution or disciplinary action, consult with legal counsel before attempting to debrief the individual.

e. It is sometimes useful to have the person being debriefed sign a statement acknowledging the debriefing and his or her understanding of its contents. The nature and format of the statement is left to the discretion of the local security official so as to allow

flexibility in meeting the requirements of a particular incident. If the person refuses to sign a debriefing statement when asked, this fact and his or her stated reasons for refusing will be made a matter of record in the inquiry.

10-106 Management and Oversight

a. The DoD Components shall establish necessary reporting and oversight mechanisms to ensure that inquiries/investigations are conducted when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problems. Inquiries/investigations and management analyses of security incidents must consider possible systemic shortcomings that may have caused or contributed to the incident. The effectiveness of activity security procedures, security education, supervisory oversight of security practices, etc., should be considered in determining causes and contributing factors. The focus of management response to security incidents should be to eliminate or minimize the probability of further incidents occurring. Appropriate disciplinary action or legal prosecution, discussed in Section 5 of Chapter 1, is sometimes one means of doing this, but the broader focus on prevention must not be lost. Simple disciplinary action—without consideration of what other factors may have contributed to the situation—should not be considered an acceptable response to a security incident.

b. Each DoD Component **shall** establish a system of controls and internal procedures to ensure that damage assessments are conducted when required and that their results are available as needed.

10-107 Additional Investigation

Additional investigation -- beyond what is required by this chapter -- may be needed to permit application of appropriate sanctions for violation of regulations, criminal prosecution, or determination of effective remedies for discovered **vulnerabilities**. The inquiry required by this chapter may serve as a part of these investigations, but notification of originators **shall** not be delayed pending completion of these additional investigations.

10-108 Unauthorized Absences

When an individual who has had access to classified information is absent without authorization, the head of the activity or security manager shall determine if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting counterintelligence organization **shall** be notified. The scope and depth of this inquiry will depend on the length of the absence and the sensitivity of the classified information involved.

APPENDIX A

REFERENCES

The references mentioned elsewhere in this Regulation are listed in numeric order (excluding classification abbreviations), grouped as follows:

Public Laws, Statutes and Executive Orders
DoD Directives and Instructions
Other DoD Publications
Other Agencies' Publications

Public Laws, Statutes, and Executive Orders

Executive Order 10964, *Safeguarding Official Information in the Interest of the Defense of the United States*, September 22, 1961

Executive Order, 12065, *National Security Information*, June 28, 1978

Executive Order 12333, *United States Intelligence Activities*, December 4, 1981

Executive Order 12356, *National Security Information*, April 6, 1982

Executive Order 12958, *Classified National Security Information*, April 20, 1995

Executive Order 12972, *Amendment to Executive Order 12958*, September 21, 1995

Title 5, U.S.C., Section 552, as amended (Public Law 104-231, 110 stat. 2422), The Freedom of Information Act

Title 5, U. S.C., Section 552a, (Public Law 93-579), *The Privacy Act of 1974*

Title 10, U. S. C., Sections 119 and 128, *Special Access Programs*

Title 15, U.S.C. Sections 271 et seq., *Computer Security Act of 1987*

Title 18, U. S.C., Section 1386, *Crimes and Criminal Procedure*, 1982

Title 31, U. S.C., Section 9701 (Title 5, *Independent Offices Appropriation Act*)

Title 35, U. S.C., Sections 181-188, *The Patent Secrecy Act of 1952*

Title 39, U.S.C., Section 320.6, *Postal Services, as amended*

Title 42, U. S.C., Sections 2011-., *Atomic Energy Act of August 30, 1954, as amended*

Title 44, U. S. C., Chapters 21,31 and 33, *Federal Records Act*

Title 50, U. S.C., Section 401, *Central Intelligence Agency Information Act*

Title 50, U. S.C., Section 403, *National Security Act of 1947*

DoD Directives and Instructions

DoD Directive 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*, " February 17, 1989

DoD Directive 5000.1, *Defense Acquisition*, March 15, 1996

DoD Directive 5010.38, *Management Control Program*, August 26, 1996

DoD Directive 5015.2, *Records Management Program*, March 22, 1991

DoD Directive 5030.47, *National Supply System*, May 27, 1971

DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoD Directive 0-5205.7, *Special Access Program (SAP) Policy*, January 4, 1989

DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, January 12, 1978

DoD Directive 5210.56, *Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Enforcement and Security Duties*, February 25, 1992

DoD Directive 5210.83, *Department of Defense Unclassified Controlled Nuclear Information*, November 15, 1991

DoD Directive 5220.22, *Department of Defense Industrial Security Program*, December 8, 1980

DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, June 16, 1992

DoD Directive 5230.20, *Visits and Assignment of Foreign Representatives*, April 24, 1992

DoD Directive 5230.24, *Distribution Statements on Technical Documents*, March 18, 1987

DoD Directive 5400.4, *Provision of Information to Congress*, January 30, 1978

DoD Directive 5405.2, *Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses*, July 23, 1985

DoD Directive 5535.2, *Delegations of Authority to Secretaries of the Military Departments - Inventions and Patents*, October 16, 1980

DoD Instruction 5240.4, *Reporting of Counterintelligence and Criminal Violations*, September 22, 1992

DoD Instruction 5240.11, *Damage Assessments*, December 23, 1991

DoD Directive 7650.1, *General Accounting Office Access to Records*, August 26, 1982

DoD publications

Department of Defense/Government Printing Office Secrecy Agreement, 1981

DoD 5000.2-R, *"Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated information Systems (MAIS) Acquisition Programs*, March 1996, authorized by DoD 5000.1, *Defense Acquisition*, March 15, 1996

DoD C-5 105.21 -M-1, *Sensitive Compartmented Information (SCI) Administrative Security Manual*, March 1995(U), authorized by DoD Directive 5105.21, *Defense Intelligence Agency*, May 19, 1977

DoD TS-5 105.21-M-2, *Sensitive Compartmented Information (SCI) Security Manual - Communications Intelligence (COMINT) Policy* (U), July 1985, authorized by DoD Directive 5105.21, *Defense Intelligence Agency*, May 19, 1977

DoD TS-5 105.21-M-3, *Sensitive Compartmented Information (SCI) Security Manual - TK Policy* (U), November 1985 (U), authorized by DoD Directive 5210.21, *Defense Intelligence Agency*, May 19, 1977

DoD 5200. 1-I, *DoD Index of Security Classification Guides*, September 1995, authorized by DoD Directive 5200.1, December 13, 1996

DoD 5200.2-R, *DoD Personnel Security Program Regulation*, January 1987, authorized by DoD Directive 5200.2, *Department of Defense Personnel Security Program (DoDSP)*, May 6, 1992

DoD 5200.33-R, *Defense Courier Service Regulation*, January 5, 1995, authorized by DoD Directive 5200.32, December 7, 1994

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995 and its supplements, authorized by DoD Directive 5220.22, *DoD Industrial Security Program*, December 8, 1980,

DoD 5220.22-R, *Industrial Security Regulation*, December 1985, authorized by DoD Directive 5220.22, *DoD Industrial Security Program*, December 8, 1980

DoD 5400.1 1-R, *Department of Defense Privacy Program*, August 1983, authorized by DoD Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982

Other Agencies' Publications

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29, **Codeword**, *Nickname, and Exercise Term Report*, February 1, 1996

Director of Central Intelligence Directive 3/29, *Controlled Access Program Oversight Committee*, June 2, 1995

Joint Chiefs of Staff Instruction 3250.1, *Policy Guidance for Sensitive Airborne and Maritime Surface Reconnaissance Operations*, May 6, 1994

Military Handbook 1013I1A, *Design Guidelines for Physical Security of Facilities*, October 9, 1987

National Communications Security Instruction (NACSI) 4009, *Protected Distribution Systems (U)*, December 30, 1981

National Telecommunications and Information Systems Security Instruction (NTISSI) 4001, *Controlled Cryptographic Items (U)*, March 25, 1985

National Telecommunications and Information Systems Security Instruction (NTISSI) 0-4003, *Reporting Communications Security (COMSEC) Insecurities*, December 2, 1991

National Telecommunications and Information Systems Security Instruction (NTISSI) C-4004, *Routine Destruction and Emergency Protection of Communications Security (COMSEC) Material*, March 11, 1987

Office of Management and Budget Circular, A- 123, Revised, *Management Accountability and Control*, June 21, 1995

U.S. Security Authority for NATO, 1-69, North Atlantic Treaty Organization (NATO) Security program (Enclosure 2 to DoD Directive 5100.55, U.S. *Security Authority for North Atlantic Treaty Organization Affairs*, April 21, 1982

APPENDIX B

DEFINITIONS

1. **Access.** The ability and opportunity to obtain knowledge of classified information.

2. **Acknowledged Special Access Program.** A SAP whose existence is known, to include association with another classified program which is publicly acknowledged.

3. **Agency.** An organization specified as such in E.O. 12958, as amended by E.O. 12972. Within the Department of Defense, this term includes the Department of Defense and the Departments of the Army, Navy, and Air Force.

4. **Applicable Associated Markings.** Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the “classified by” line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

5. **Automated Information System.** An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

6. **Automatic declassification.** The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under E.O. 12958.

7. **Carve-Out.** A classified contract for which the Defense Investigative Service has been relieved of inspection responsibility in whole or in part.

8. **Classification.** The actor process by which information is determined to be classified information.

9. **Classification Guidance.** Any instruction or source that prescribes the classification of specific information.

10. **Classification Guide.** A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

11. **Classified National Security Information.** (Or

“Classified Information”). Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

12. **Classifier.** An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

13. **Code Word.** A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher.

14. **Collateral Information.** Information identified as National Security Information under the provisions of E.O. 12958 but which is not subject to enhanced security protection required for SAP Information.

15. **Communications Security (COMSEC).** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

16. **Compromise.** An unauthorized disclosure of classified information.

17. **Confidential Source.** Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

18. **Continental United States (CONUS).** United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

19. **Controlled Cryptographic Item (CCI).** A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled.

(Equipments and components so designated bear the designator “Controlled Cryptographic Item” or ‘CCL’)

20. Critical Nuclear Weapon Design Information (CNWDI). That Top Secret Restricted Data or Secret Restricted Data **revealing** the theory of operation or design of the components of a **thermo-nuclear** or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fusing, and **firing** systems; limited life components; and total contained quantities of fissionable, fissionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test, or replace.

21. Cryptanalysts. The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption.

22. Cryptography. The branch of cryptology which treats the principles, means, and methods of designing and using **cryptosystems**.

23. Cryptology. The branch of knowledge which treats the principles of cryptography and **cryptanalytics**; and the activities involved in producing signals intelligence (**SIGINT**) and maintaining communications security (**COMSEC**).

24. Damage to the National Security. **Harm** to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

25. Declassification. The authorized change in the status of information from classified information to unclassified information.

26. Declassification Authority. a. The **official** who authorized the original classification, if that **official** is still serving in the same position; b. the originator’s current successor in function; c. a supervisory **official** of either; or **d.officials** delegated declassification authority in writing by the agency head or the senior agency official.

27. Declassification Guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

28. Derivative Classification. The process of determining whether information has already been originally classified and, if it has, ensuring that it

continues to be identified as classified by marking or similar means when included in newly created material.

29. Document. Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

30. DoD Component. The Office of the Secretary of Defense (**OSD**), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense Agencies.

31. Downgrading. A determination that information classified at a specified level shall be classified at a lower level.

32. Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

33. File series. Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a **filing** system or maintained as a unit because it pertains to the same function or activity.

34. Foreign Government Information. a. Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; b. information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or c. information received and treated as “Foreign Government Information” under the terms of a predecessor order to E.O. 12958.

35. Formerly Restricted Data. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

36. Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United

States Government. “Control” means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

37. **Information Security.** The system of policies, procedures, and requirements established under the authority of **E.O. 12958** to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

38. **Infraction.** Any knowing, willful, or negligent action contrary to the requirements of **E.O. 12958** or its implementing directives that does not comprise a “violation,” as defined in paragraph 69 below.

39. **Integrity.** The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

40. **Intelligence Activity.** An activity that an agency within the Intelligence Community is authorized to conduct under **E.O. 12333**.

41. **Mandatory Declassification Review.** Review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of **E.O. 12958**.

42. **Material.** Any product or substance on or in which information is embodied.

43. **Multiple Sources.** Two or more source documents, classification guides, or a combination of both.

44. **National security.** The national defense or foreign relations of the United States.

45. **Need-to-know.** A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

46. **Network.** A system of two or more computers that can exchange data or information.

47. **Nickname.** A nickname is a combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

48. **Original Classification.** An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

49. **Original Classification Authority.** An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

50. **Permanent Historical Value.** Those records that have been identified in an agency records schedule as being permanently valuable.

51. **Prospective Special Access Program (P-SAP).** A DoD program or activity for which enhanced security measures have been proposed and approved to facilitate security protections prior to establishing the effort as a DoD SAP.

52. **Protective Security Service.** A transportation protective Service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (**MTMC**) to transport **SECRET** shipments. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier’s aircraft in connection with flight, provided the shipment is loaded into a compartment that is not accessible to an unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft that is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

53. **Regrade.** To raise or lower the classification assigned to an item of information.

54. **Restricted Data.** All data concerning a. design, manufacture or utilization of atomic weapons; b. the production of special nuclear material; or c. the use of special nuclear material in the production of **energy**, but shall not include data declassified or removed from the Restricted Data category under Section 142 of the Atomic Energy Act of 1954, as amended.

55. **Safeguarding.** Measures and controls that are prescribed to protect classified information.

56. **Security Clearance.** A determination that a person is eligible under the standards of DoD 5200.2-R for access to classified information.

57. **Security In-Depth:** A determination by the senior agency official that a facility’s security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to use of perimeter fences,

employee and visitor access controls, use of an Intrusion Detection System, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

58. **Self-Inspection.** The internal review and evaluation of individual agency activities and the agency **as** a whole with respect to the implementation of the program established under **E.O.** 12958 and its implementing directives.

59. **Senior Agency Official.** An official appointed by the Secretary of Defense, Secretary of the Army, Secretary of the Navy, or Secretary of the Air Force under the provisions of Section 5.6(c) of **E.O.** 12958.

60. **Senior Official.** An official appointed by the head of a DoD Component to be responsible for direction and administration of the Information Security Program. (Note: In the Departments of Defense, Army, Navy, and Air Force, this **official** will also be the “Senior Agency **Official**” as defined above.

61. **Sensitive Compartmented Information.** Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence.

62. **Special Access Program (SAP).** Any DoD program or activity (as authorized in E. O. 12958), employing enhanced security measures (e.g. safeguarding, access requirements, etc.) exceeding those normally required for collateral information at the same **level** of classification shall be established, approved, and managed as a DoD SAP.

63. **Special Activity.** An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does

not include diplomatic activities or the collection and production of intelligence or related support functions.

64. **Systematic Declassification Review.** The review for declassification of classified information contained in records that have been determined by the Archivist of the United States (“Archivist”) to have permanent historical value in accordance with chapter 33 of title 44, United States Code, and is exempted from the automatic declassification provisions of section 3 of Chapter 4 of this Regulation.

65. **Telecommunications.** The preparation, transmission, or communication of information by electronic means.

66. **Unacknowledged Special Access Program.** A SAP, the existence of which is not acknowledged, **affirmed**, or made known to any person not authorized for access.

67. **Unauthorized disclosure.** A communication or physical transfer of classified information to an unauthorized recipient.

68. **Upgrade.** To raise the classification of an item of information from one level to a higher one.

69. **Violation.** a.) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; b. any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of **E.O.** 12958 or its implementing directives; or c.) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of **E.O.** 12958.

70. **Waived Special Access Program.** A SAP for which the Secretary of Defense has waived applicable reporting requirements of Section 119 of title 10, U. S. C., is identified as a “Waived SAP” and therefore has more restrictive reporting and access controls.

APPENDIX C

CONTROLLED UNCLASSIFIED INFORMATION

Section 1

Introduction

1-100 General

a. The requirements of the Information Security Program apply only to information that requires protection to prevent damage to the national security and has been classified in accordance with E.O. 12958 or its predecessors. There are other types of information that require application of controls and protective measures for a variety of reasons. This information is known as “unclassified controlled information.” Since classified information and unclassified controlled information exist side-by-side in the work environments-often in the same documents-this appendix is provided as an attempt to avoid confusion and promote proper handling. It covers several types

of unclassified controlled information, and provides basic information about the nature of this information and the procedures for identifying and controlling it. In some cases, the appendix refers to other DoD Directives that provide more detailed guidance.

b. The types of information covered in this appendix include “For Official Use Only” information, “Sensitive But Unclassified” (formerly “Limited Official Use”) information, “DEA Sensitive Information,” “DoD Unclassified Controlled Nuclear Information,” “Sensitive Information” as defined in the Computer Security Act of 1987, and information contained in technical documents.

Section 2

For Official Use Only Information.

2-200 Description

a. “For Official Use Only (FOUO)” is a designation that is applied to *unclassified* information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions which may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

(1) Information which is currently and properly classified.

(2) Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, “high” and “low.” The “high” profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The “low” profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)

(3) Information specifically exempted by a statute establishing **particular** criteria-for withholding. The language of the statute must clearly state that the

information will not be disclosed.

(4) Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government’s ability to obtain like information in the future, or protect the government’s interest in compliance with program effectiveness.

(5) Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

(6) Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

(7) Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source, (e) disclose investigative

techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.

(8) Certain records of agencies responsible for supervision of financial institutions.

(9) Geological and geophysical information concerning wells.

b. Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. “For **Official Use Only**” is applied to information that is exempt under one of the *other* eight categories. So, by definition, information must be unclassified in order to be designated **FOUO**. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that (1) information cannot be classified and FOUO at the same time, and (2) information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

c. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories *and* there must be a legitimate Government purpose served by withholding it. **Simply** because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still qualify for withholding under the **FOIA**.

2-201 Markings

a. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

b. Unclassified documents and material containing FOUO information shall be marked as follows:

(1) Documents will be marked “FOR OFFICIAL USE ONLY” at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).

(2) Pages of the document that contain FOUO information shall be marked “FOR OFFICIAL USE

ONLY” at the bottom.

(3) Material other than paper documents (for example, slides, computer **media**, films, etc.) shall bear markings which alert the holder or viewer that the material contains FOUO information.

(4) FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that **non-DoD** holders understand the status of the information. A statement similar to this one should be used:

This document contains information
exempt from mandatory disclosure under
the **FOIA**.

Exemption(s) _ apply.

c. Classified documents and material containing FOUO information shall be marked as required by Chapter V of this regulation, with FOUO information identified as follows:

(1) Overall markings on the document shall follow the rules in Chapter 5. No special markings are required on the face of the document because it contains FOUO information.

(2) Portions of the document shall be marked with their classification as required by Chapter 5. If there are unclassified portions that contain FOUO information, they shall be marked with “**FOUO**” in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the “**FOUO**” is an acceptable substitute for the normal “U.”

(3) Pages of the document that contain classified information shall be marked as required by Chapter 5. Pages that contain FOUO information but no classified information will be marked “FOR OFFICIAL USE ONLY” at the top and bottom.

d. Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one: “FOR OFFICIAL USE ONLY Attachment.”

e. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation “**FOUO**” before the beginning of the text.

2-202 Access to FOUO Information

FOUO information may be disseminated within the DoD Components and between officials of the DoD

Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to **officials** in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. (Special restrictions may apply to information covered by the Privacy Act.) Release of FOUO information to Members of Congress is covered by DoD Directive 5400.4, and to the General Accounting **Office** by DoD Directive 7650.1.

2-203 **Protection of FOUO Information**

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. **After** working hours, FOUO information shall be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked desks, file cabinets, bookcases, locked rooms, or similar items.

b. FOUO documents and material may be transmitted via first class mail, parcel post or—for bulk shipments—fourth class mail. Electronic transmission of FOUO information (voice, data or facsimile) should be by approved secure communications systems whenever practical.

c. Record copies of FOUO documents shall be disposed of in accordance with the Federal Records Act (44 **U.S.C.** 33) and Component records management directives. Non-record FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

2-204 **Further Guidance**

Further guidance on one type of FOUO information is contained in DoD 5400.1 I-R, Department of Defense Privacy Program.

Section 3

Sensitive But Unclassified and Limited Official Use Information

3-300 **Description**

Sensitive But Unclassified (**SBU**) information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act. Before 26 May 1995, this information was designated and marked “Limited Official Use (LOU).” The LOU designation will no longer be used.

3-301 **Markings**

The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls.

When SBU information is included in DoD documents, they shall be marked as if the information were For Official Use Only. There is no requirement to remark existing material containing SBU information.

3-302 **Access to SBU Information**

Within the Department of Defense, the criteria for allowing access to SBU information are the same as those used for FOUO information.

3-303 **Protection of SBU Information**

Within the Department of Defense, SBU **information** shall be protected as required for FOUO **information**.

Section 4

Drug Enforcement Administration Sensitive Information

4-400 **Description**

DEA Sensitive information is unclassified information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The Administrator and certain other officials of the DEA have been authorized to designate information as DEA Sensitive; the Department of Defense has agreed to implement

protective measures for DEA Sensitive information in its possession. Types of information to be protected include:

a. Information and material that is investigative in nature;

b. Information and material to which access is restricted by law;

c. Information and material that is critical to the

operation and mission of the DEA; and

d. Information and material the disclosure of which would violate a privileged relationship.

4-401 Markings

a. **Unclassified documents containing DEA Sensitive information shall be marked “DEA Sensitive” at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).**

b. In unclassified documents, each page containing DEA Sensitive information shall be marked “DEA Sensitive” top and bottom. Classified documents containing DEA Sensitive information shall be marked as required by Chapter 5, except that pages containing DEA Sensitive information but no classified information will be marked “DEA Sensitive” top and bottom.

c. Portions of DoD documents that contain DEA Sensitive information **shall** be marked “(DEA)” at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA Sensitive information, the “**DEA**” marking shall be included along with the parenthetical classification marking.

4-402 Access to DEA Sensitive Information

Access to DEA Sensitive information shall be granted only to persons who have a valid need-to-know for the information. A security clearance is not required. DEA Sensitive information in the possession of the Department of Defense may not be released outside the Department without authorization by the DEA.

4-403 Protection of DEA Sensitive Information

a. **DEA Sensitive material may be transmitted within CONUS by first class mail. Transmission outside CONUS must be by a means approved for transmission of Secret material. Non-government package delivery and courier services may not be used.** The material shall be enclosed in two opaque envelopes or containers, the inner one marked “DEA Sensitive” on both sides. Electronic transmission of DEA Sensitive information within CONUS should be over secure communications circuits whenever possible; transmission outside CONUS must be over approved secure communications circuits.

b. Reproduction of DEA Sensitive information and material shall be limited to that required for operational needs.

c. DEA Sensitive material shall be destroyed by a means approved for destruction of Confidential material.

Section 5

DoD Unclassified Controlled Nuclear Information

5-500 Description

DoD Unclassified Controlled Nuclear Information (DoD UCNI) is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (**SNM**), equipment, or facilities. Information is Designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals to whom they have delegated the authority.

5-501 Markings

a. Unclassified documents and material containing DoD UCNI shall be marked as follows:

(1) The face of the document and the outside of the back cover (if there is one) shall be marked “DoD Unclassified Controlled Nuclear Information.”

(2) Portions of the document that contain DoD UCNI shall be marked with “(DoD UCNI)” at the beginning of the portion.

b. Classified documents and material containing DoD UCNI shall be marked in accordance with Chapter V, except that:

(1) Pages with no classified information but containing DoD UCNI shall be marked “DoD **Unclassified** Controlled Nuclear Information” at the top and bottom.

(2) Portions of the document that contain DoD UCNI shall be marked with “(DoD UCNI)” at the

beginning of the portion-in addition to the classification marking, where appropriate.

c. Material other than paper documents (for example, slides, computer **media**, films, etc.) shall bear markings that **alert** the holder or viewer that the material contains DoD UCNI.

d. Documents and material containing DoD UCNI and transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that **non-DoD** holders understand the status of the information. A statement similar to this one should be used:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR
INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE
(5 U.S.C. 552(b)(3), as authorized by .10 U.S.C. 128)

e. Transmittal documents that have DoD UCNI attachments shall bear a **statement**: “The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI).”

5-502 **Access to DoD UCNI**

Access to DoD UCNI shall be granted only to per-

sons who have a valid need-to-know for the information and are specifically eligible for access under the provisions of DoD Directive 5210.83, Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI).

5-503 **Protection of DoD UCNI**

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, DoD UCNI may be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked buildings, rooms, desks, **file** cabinets, bookcases, or similar items.

b. DoD UCNI may be transmitted by first class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DoD UCNI shall be over approved secure communications circuits.

c. Record copies of DoD UCNI documents shall be disposed of in accordance with the Federal Records Act (44 U.S.C. 33) and Component records management directives. Non-record DoD UCNI documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

Section 6

Sensitive Information (Computer Security Act of 1987)

6-600 **Description**

a. **The Computer Security Act of 1987 established requirements** for protection of certain information in Federal Government automated information systems (AIS). This information is referred to as “sensitive” information, defined in the Act as: “Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”

b. Two aspects of this definition deserve attention. First, the **Act** applies only to unclassified information that deserves protection. Second, unlike most other programs for protection of information, the Act is concerned with protecting the availability and integrity, as well as the confidentiality of information. Much of the

information which fits the Act’s definition of “sensitive” falls within the other categories of information discussed in this Appendix. Some does not.

6-601 **Markings**

There is no specific marking authorized for designation of “sensitive” information. If the information fits within one of the other categories of information described in this Appendix, the appropriate marking requirements apply.

6-602 **Access to Sensitive Information**

If sensitive information falls within one of the other categories of information described in this Appendix, the specific limitations on access for the appropriate category **shall** be applied. If it does not, access to the information shall be limited only to those with a valid need for such access in order to perform a legitimate organizational function, as dictated by common-sense principles of security management.

6-603 Protection of Sensitive Information

Information on DoD AIS systems that is determined to be “sensitive” within the meaning of the Computer Security Act of 1987 shall be provided protection that is:

a. Determined after thorough consideration of the value and sensitivity of the information and the probable adverse impact of loss of its availability, integrity or confidentiality;

b. In compliance with applicable DoD policy and requirements for security of information within automated systems;

c. Commensurate with the degree of protection required for the category of information described in this Appendix to which it belongs (if any); and

d. Based on sound application of risk management techniques and procedures.

6-604 Further Guidance

Further guidance is found in DoD Directive 5200.28, Security Requirements for Automated Data Processing (**ADP**) Systems, and related publications.

Section 7

Technical Documents

7-700 General

DoD Directive 5230.24 requires distribution statements to be placed on technical documents, both **classified** and unclassified. **These** statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case-by-case exceptions to distribution limitations imposed by the statements.

7-701 Text of the Statements

Distribution Statement A

Approved for public release; distribution is unlimited.

Distribution Statement B

Distribution authorized to U.S. Government agencies **only**; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement C

Distribution authorized to US Government agencies and their contractors; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement D

Distribution authorized to the DoD and US DoD contractors only; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement E

Distribution authorized to DoD Components only; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office]. .

Distribution Statement F

Further distribution only as directed by [controlling DoD office] or higher DoD authority; [date].

Distribution Statement X

Distribution authorized to US Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; [date].

Controlling DoD office is [controlling DoD office].

APPENDIX D

SPECIAL PROCEDURES FOR USE IN SYSTEMATIC AND MANDATORY REVIEW OF CRYPTOLOGIC INFORMATION

1. General guideline: **Cryptologic** information uncovered in systematic or mandatory review for declassification of 25-year old government records is not to be declassified by other than the National Security Agency. The information may concern or reveal the processes, techniques, operations, and scope of signals intelligence (**SIGINT**), which consists of communications intelligence (**COMINT**), electronic intelligence (**ELINT**), and foreign instrumentation signals intelligence (**FISINT**), or it may concern the components of Information Security (**INFOSEC**) which consists of communications security (**COMSEC**) and computer security (**COMPUSEC**), including the communications portion of cover and deception plans. Much **cryptologic** information is also considered “Foreign Government Information” as defined in Para. 1. l(d) of the Executive Order 12958.

2. Recognition of cryptologic information may not always be an easy task. There are several broad classes of **cryptologic** information, as follows: .

a. Those that relate to **INFOSEC**: In documentary form, they provide **COMSEC/COMPUSEC** guidance or information. Many **COMSEC/COMPUSEC** documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing telecommunications security (**TSEC**) nomenclature and crypto keying material for use in enciphering communications and other **COMSEC/COMPUSEC** documentation such as the National Telecommunications and Information Systems Security Committee or its predecessor organization, **COMSEC/COMPUSEC** Resources Program documents, **COMSEC** Equipment Engineering Bulletins, **COMSEC** Equipment System Descriptions, and **COMSEC** Technical Bulletins.

b. Those that relate to **SIGINT**: These appear as reports in various formats that bear security classifications., frequently followed by five-letter codewords, for example, World War II’s **ULTRA**, and often carry warning caveats such as “This document contains codeword material” and “Utmost secrecy is **necessary**...” or “Handle Via **COMINT** Channels Only” or **HVCCO**’ or “**CCO**.” Formats may appear as messages having addresses, “from” and “to” sections, and as summaries with **SIGINT** content with or without other kinds of intelligence and comment.

c. Research, development, test, life cycle support, planning, and evaluation reports and information that relates to either **COMSEC**, **COMPUSEC**, or **SIGINT**.

3. Some commonly used words that help to identify cryptologic documents and materials are “cipher,” “code,” “codeword,” communications intelligence,” or “**COMINT**,” “special

intelligence, “ “communications security,” or “COMSEC,” “ “computer security or **COMPUSEC**,” **cryptanalysis**,” crypto,” cryptography,” “cryptosystem,” “cipher,” “decipher,” “decode,” “**decrypt**,” “direction finding,” “ “electronic intelligence” or “ELINT,” “electronic security,” “encipher,” “encode,” “encrypt,” “ “foreign instrumentation signals intelligence” or “**FISINT**” pr “**FIS**,” “telemetry” information systems security” or “TNFOSEC,” “intercept,” :**key book**,” “one-time-pad,” “ “bookbreaking,” “ “signals intelligence” or “SIGINT,” “signals security,” “**TEMPEST**,” and “traffic analysis” or “TA.”

4. Special procedures apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information.

a. **INFOSEC** (COMSEC and COMPUSEC) Documents and Materials.

(1) If records or materials in this category **are** found in agency or department component files that are not under INFOSEC control, refer them to the senior COMSEC/COMPUSEC authority of the agency or department concerned or return them, by appropriate channels, to the address in item 4.c, below.

(2) If the COMSEC/COMPUSEC information has been incorporated into other documents by the receiving agency, that information must be referred to the National Security Agency/Chief Central Security Service (**NSA/CSS**) for review before declassification occurs.

b. **SIGINT** (COMINT, ELINT, and FISINT) Information.

(1) If the **SIGINT** information is contained in a document or record originated by a U.S. Government cryptologic organization and is in the files of a **non-cryptologic** agency or department, such material will not be declassified. The material maybe destroyed unless the holding agency’s approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the **NSA/CSS** for systematic review for declassification when it becomes 25-years old or older.

(2) If the **SIGINT** information has been incorporated by the receiving agency into documents it produces, referral of the **SIGINT** information to the **NSA/CSS** for review is necessary prior to any declassification action.

c. COMSEC/COMPUSEC or **SIGINT** information which requires declassification by the **NSA/CSS** should be sent to:

Director, National Security Agency/
Chief, Central Security Service
AITN: Information Policy Staff (**N5P6**)
Fort George G. Meade, MD 20755-6000

APPENDIX E

CONTROL OF DISSEMINATION OF INTELLIGENCE INFORMATION

(TO BE PROVIDED AT A LATER DATE

APPENDIX F

Equivalent Foreign Security Classifications

Country	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Albania	TEPER SEKRET	SEKRET	IMIREBESUESHEM	I KUFIZUAR
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Balkans	STROGO POVERLJIVO State <u>SECRET</u> DRZAVA TAJNA	TAJNO Military <u>SECRET</u> VOJNA TAJNA	POVERLJIVO	
Belgium(French)	TRES SECRET	SECRET	CONFIDENTIAL	DIFFUSION RESTRAINTS
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Bulgaria	STROGO SEKRETO	SEKRETEN/ SEKRETNO	POVERITELEN/ POVERITELNO	OGRANICHE (as in
Limited)				NEPOZVOLEN (Illicit) ZABRANEN (Forbidden)

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
Columbia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENTIAL RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENTIAL	
Croatia	NAJVECI TAJNITAJNI	TAJNI	POVERLJIV	OGRANC IEN
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENTIAL	RESERVADO
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN			
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIAL	DIFFUSION RESTREINTE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	
Greece	AKPΩΣ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Guatamala	ALTO SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Haiti		SECRET	CONFIDENTIAL	
Honduras	SUPER SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Hungary	SZIGOR'UAN TITKOS	TITKOS	BIZALMAS	
Iceland	ALGJORTI	TRUNADARMAL		
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BENKOLI SERRI	SERRI	KHEILI MAHRAMANEH	MAHRAMANEH
Iraq (English Translation)	ABSOLUTELY SECRET	SECRET		LIMITED
Ireland(Gaelic)	AN-SICREIDEACH	SICREIDEACH	RUNDA	SRIANTA
Israel	SODI BEYOTER	SODI	SHAMUR	MUGBAL
Italy	SEGRETISSIMO	SECRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU	GOKUHI	HI	TORIATSUKAICHUI
Jordan	MAKTUM JIDDAN	MAKTUM	SIRRI	MAHDUD
Kazakstan	Use Russian equivalent			

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Korea	I KUP PI MIL	II KUP PI MIL	III KUP PI MIL	
Kyrgyzstan	Use Russian equivalent			
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIAL	
Moldovan (May also use Russian Equivalent)	ULTRASECRET	SECRET	CONFIDENTIAL OR SECRET	RESTRINS
Mexico	ALTO SECRETO	SECRETO	CONFIDENTIAL	RESTRINGIDO
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or VERTROUWELIJK	DIENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELL	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENTIAL	RESERVADO

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	TAJNY SPECJALNEGO	TAJNY	POUFNY	
Portugal	MUITO SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Romanian	uLTRASECRET	SECRET	CONFIDENTIAL OR SECRET	RESTRINS
Russian	COBEOWEHHO	CEKPETHO		
Saudi Arabia	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI RESTRICTED
Spain	MAXIMO SECRETO	SECRETO	CONFIDENTIAL	DIFFUSION LIMITADA
Sweden (Red Borders)	HEMLIG	HEMLIG		
Switzerland	(Three languages. TOP SECRET has a registration number to distinguish it from SECRET AND CONFIDENTIAL)			
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIAL DEFENSE	DIFFUSION RESTREINTE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH	
Italian	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Taiwan	(No translation in English characters)			
Tajikistan	Use Russian equivalent			

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Turkey	COK GIZLI	GIZLI	OZEL	HIZMET OZEL
Turkmenistan	Use Russian equivalent			
Ukraine	TSILKOM SEKRETNE	SEKRETNO	KONFIDENTSIAL 'NO	DLYA
Union of South Africa	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK
United Arab Republic (Egypt)	TOP SECRET	VERY SECRET	SECRET	OFFICIAL
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
URUGUAY	ULTRA SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Uzbekistan	Use Russian equivalent			
Viet Nam(French) (Vietnamese)	TRES SECRET TOI-MAT	SECRET DEFENSE MAT	CONFIDENTIAL DEFENSE KIN	DIFFUSION RESTREINTE TU MAT

Note: The classifications given above represent the nearest comparable designation that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classification.

APPENDIX G

PHYSICAL SECURITY STANDARDS

A. Vault and Secure Room Construction Standards

1. Vault

a. Floor and Walls. Eight inches of concrete reinforced to meet current standards. Walls are to extend to the underside of the roof slab above.

b. Roof. Monolithic reinforced-concrete slab of **thickness to be** determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling must be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors and walls

d. Vault door and frame unit should conform to Federal Specification AA-D-2757 Class 8 vault door, or Federal Specification AA-D-600 Class 5 vault door.

2. Secure Room

a. The walls, floor, and roof construction of secure rooms must be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, **hard**-board, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. **Walls** shall be extended to the true ceiling and attached with permanent construction materials,

with mesh or 18 gauge expanded steel screen.

b. Ceiling. The ceiling **shall** be constructed of plaster, gypsum, wallboard material, hardware or any other acceptable material.

c. Doors. The access door to the room **shall** be substantially constructed of wood or metal. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Door should be equipped with a built-in GSA-approved combination lock meeting Federal Specification **FF-L-2740**.

d. Windows. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, **shall** be constructed from or covered with materials that will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

e. Openings. Utility openings such as ducts and vents should be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches will be hardened in accordance with Military Handbook 1013/1 A.

B. Intrusion Detection System (IDS) Standards

1. An IDS must detect an unauthorized penetration in the secured area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE)

b. Security forces

c. Operating procedures

2. System Functions

a. IDS components operate as a system with the following four distinct phases:

(1) Detection

(2) Communications

(3) Assessment

(4). Response

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone" at the monitor station. This shall be used as the definition of an alarmed zone for purposes of this Regulation.

(2) **Reporting:** The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communication scheme. This tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals. When an alarms occur, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) **Assessment:** The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) **Response:** The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

3 Threat, Vulnerability and Acceptability

a. As determined by the commander all areas that reasonably afford access to the container, or where classified data is stored should be protected by IDS unless continually occupied. Prior to the installation of an IDS, commanders shall consider the threat, **vulnerabilities**, in-depth security measures and shall perform a risk analysis.

b. **Acceptability of Equipment:** All IDE must be **UL-listed**, (or equivalent) and approved by the DoD Component or government contractor. Government installed, maintained, or furnished systems are acceptable.

4. Transmission and Annunciation

a. **Transmission Line Security:** When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(1) **Class I:** Class I line security is the achieved through the use of DES or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

(2) **Class II:** Class II line supervision refers to systems in which the transmission is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum 6 month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. **Internal Cabling:** The cabling between the sensors and the PCU should be dedicated to IDE and must comply with national and local code standards.

c. **Entry Control Systems:** If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion alarms.

d. **Maintenance Mode:** When an alarm zone is placed in the maintenance mode, condition shall be signaled automatically to the monitor station. The signal must appear as an alarm, or maintenance message at the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the **monitor**-station throughout the period of maintenance. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to one second per occurrence.

e. **Annunciation of Shunting or Masking Condition:** Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f. **Indications of alarm status** shall be revealed at the monitoring station and optionally within the confines of the secure area.

g. **Power Supplies:** Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(1) **Emergency Power:** Emergency power shall consist of a protected **independent** backup power source that provides a minimum of 4 hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The

manufacturer's periodic maintenance schedule shall be followed and results documented.

(2) Power Source and Failure Indication: An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, a change in power source, and the location of the failure or change.

h. Component Tamper Protection: IDE components located inside or outside the secure area should be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection should be provided.

5. System Requirements

a. Independent Equipment: When many alarmed areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

b. Access and/or Secure Switch and PCU: No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUS must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection: Secure areas that reasonably afford access to the container or where classified data is stored should be protected with motion detection sensors; e.g., ultrasonic and passive infrared. Use of dual technology is authorized when one technology transmits an alarm condition independently

from the other technology. A failed detector shall cause an immediate and continuous **alarm** condition.

d. Protection of Perimeter Doors: Each perimeter door shall be protected by a balanced magnetic switch (BMS) that meets the standards of UL 634.

e. Windows: All readily accessible windows (within 18 feet of ground level) shall be protected by an IDS, either independently or by the motion detection sensors in the space.

f. IDS Requirements for Continuous Operations Facilities: A continuous operations facility may not require an IDS. This type of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

g. False and/or Nuisance Alarm: Any alarm signal transmitted in the absence of detected intrusion or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. **All** alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed 1 in a period of 30 days per zone.

6. Installation, Maintenance and Monitoring

a. IDS Installation and Maintenance Personnel: Alarm installation and maintenance should be accomplished by U.S. citizens who have been subjected to a trustworthiness determination in accordance with DoD 5200.2-R.

b. Monitor Station Staffing: The monitor station should be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination in accordance with DoD 5200.2-R.

C. Priorities for Replacement of Locks

[Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.]

Lock Replacement priorities In the United States and Its Territories

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	3	4
Containers (A) ¹	3	4	4	4
Containers (B)*	1	1	1	2
Crypto	1	1	2	2

Lock Replacement Priorities Outside the United States and Its Territories

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	2	2
Containers (A)	2	2	3	3
Containers (B)	1	1	1	2
Crypto	1	1	2	2
High Risk Areas	1	1	1	1

¹ 1. Located in a controlled environment where the Department of Defense has the authority to prevent unauthorized disclosure of classified information. The Government may control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

² 2. Located in an uncontrolled area without perimeter security measures.

D. Access Controls

1. Access Controls

The perimeter entrance should be under visual control at **all** times during working hours to prevent entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard **CCTV**). Regardless of the method used, an access control system shall be used on the entrance. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures at the **facility**-

a. Automated Entry Control Systems: An automated entry control system may be used to control admittance during working hours instead of visual control, if it meets the AECS criteria stated in subparagraphs 1a., and 2., below.

The automated entry control system must identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(1) ID Badges or Key Cards. The ID badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification. Personal identity verification (Biometrics Devices) identifies the individual requesting access by some unique personal characteristic, such as:

- (a) Fingerprinting
- (b) Hand Geometry
- (c) Handwriting
- (d) Retina scans
- (e) Voice recognition.

A biometrics device may be required for access to the most sensitive information.

2. In conjunction with subparagraph 1.a.(1), above, a personal identification number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or **subjected** to compromise.

3. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the ID badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access **level**

4. Protection must be established and maintained for all devices or equipment which constitute the entry control system. The level of protection may vary depending upon the type of device or equipment being protected.

a. Location where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

b. Card readers, keypads, communication or interface devices **located** outside the entrance to a controlled area shall have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels **located** within a controlled area shall require only a minimal degree of physical security protection **sufficient** to preclude unauthorized access to the mechanism

c. Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

d. Systems that use transmission lines to , carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

e. Electric strikes used in access control systems shall be heavy duty, industrial grade.

5. Access to records and information concerning encoded ID data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

6. Records shall be maintained reflecting active assignment of ID badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained

for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved and recorded.

7. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need to know and access. The Heads of DoD Components may approve the use of standardized AECS which meet the following criteria:

a. For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

b. For a Level 2 key card and PIN system, the AECS must provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

c. For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a 0.97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been

made,

8. Electric, Mechanical, or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following **manner**:

a. The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel (located within the area) will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

c. The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest classified information controlled within.

d. Electrical components, wiring included, or mechanical links (cables, rods and so on) should be accessible only from inside the area, or, if they traverse an uncontrolled area they should be secured within protecting covering to preclude surreptitious manipulation of components.

APPENDIX H

TRANSMISSION TO FOREIGN GOVERNMENTS

Classified information or material approved for release to a foreign government shall be transferred between authorized representatives of each government in compliance with the provisions of this Appendix. Each contract, agreement, or other arrangement that involves the release of classified material as freight to foreign entities **shall** either contain detailed transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials and the recipient government before release of the material. Transportation plan requirements are outlined in paragraph e., below. (See DoD TS-5105.2I-M-3 for guidance regarding **SCI**.)

a. Classified information or material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government to sign for and assume custody and responsibility on behalf of the government (hereinafter referred to as the designated government representative). This written designation shall contain assurances that such person has a security clearance at the appropriate level and that the person shall assume full security responsibility for the material on behalf of the foreign government. The recipient shall be required to execute a receipt for the material, regardless of the level of classification.

b. Classified material that is suitable for transfer by courier or postal service in accordance with this Regulation, and that cannot be transferred directly to a foreign government's designated representative shall be transmitted to:

(1) An embassy, consulate, or other official agency of the recipient government having **extraterritorial** status in the United States, or to

(2) A U.S. Embassy or a U.S. military organization in the recipient country or in a third-party country for delivery to a designated representative of the recipient government.

c. The shipment of classified material as freight via **truck**, rail, aircraft, or ship shall be in compliance with the following:

(1) DoD officials authorized to approve a

Foreign Military Sales (**FMS**) transaction that involves the delivery of U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of a proposal, consult with DoD transportation authorities (Military Traffic Management Command, Military Sealift Command, Air Mobility Command, or other, as appropriate) to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the United States shall use the Defense Transportation System (**DTS**) to deliver classified material to the recipient government. A transportation plan shall be developed by the DoD Component that prepares the Letter of Offer in coordination with the purchasing government. Security **officials** of the DoD Component that prepares the Letter of Offer shall evaluate the adequacy of the transportation plan.

(2) Classified shipments resulting from direct commercial sales must comply with the same security standards that apply to FMS shipments. To develop and obtain approval of the required transportation plan, defense contractors shall consult with the purchasing government and the DIS Regional Security Office before consummation of a commercial contract that will result in the shipment of classified material.

(3) Delivery of classified material to a foreign government at a point within the United States, its territories, or its possessions, shall be accomplished at:

(a) An embassy, consulate, or other **official** agency under the control of the recipient government.

(b) The point of origin. When a designated representative of the recipient government accepts delivery of classified U.S. material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall assure that the recipient is aware of secure means of onward movement of the classified material to its final destination, consistent with the approved transportation plan.

(c) A military or commercial port of embarkation (POE) that is recognized point of departure from the United States, its territories, or possessions, for on-loading aboard a ship, aircraft, or other carrier. In these cases, the transportation plan shall provide for U.S.-controlled secure shipment to the CONUS transshipment point and the identification of a secure

storage facility, government or commercial, at or near the POE. A DoD official authorized to transfer custody is to supervise or observe the on-loading of FMS material being transported when physical and security custody of the material has yet to be transferred formally to the foreign recipient. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper, segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility designated in the transportation plan.

(d) An appropriately cleared freight forwarder facility identified by the recipient government as its designated government representative. In these cases, a person identified as a designated government representative must be present to accept delivery of the classified material and receipt for it, to include full acceptance of security responsibility.

(4) Delivery outside the United States, its territories, or possessions:

(a) Classified U.S. material to be delivered to a foreign government within the recipient country **shall** be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the material may be delivered directly to the recipient government's designated representative upon arrival.

(b) Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the United States, or of the recipient government, that has **extraterritorial** status or otherwise is exempt from the jurisdiction of the third country. Unless the material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and deliver it to the recipient government's designated representative.

(5) Overseas Shipments

Overseas shipments of U.S. classified material shall be made only via ships, aircraft, or other carriers that are: (a) owned or **chartered** by the U.S.

Government or under U.S. registry, (b) owned or chartered by or under the registry of the recipient government, or (c) otherwise authorized by the head of the DoD Component having classification jurisdiction over the material involved. Overseas shipments of classified material shall be escorted, prepared for shipment, packaged, and stored onboard as prescribed elsewhere in this Regulation and in DoD 5220.22-R and DoD 5220.22-M.

(6) Only freight forwarders that have been granted an appropriate security clearance by the Department of Defense or the recipient government are eligible to receive, process related security documents, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of classified material, and is not required to perform security related functions, need not be cleared.

d. Foreign governments may return classified material to a U.S. contractor for repair, modification, or maintenance. At the time the material is initially released to the foreign government, the approved methods of return shipment shall be specified in the Letter of Offer and Acceptance (LOA) for FMS, the security requirements section of a direct commercial sales contract or in the original transportation plan. The contractor, upon notification of a return shipment, shall give advance notice of arrival to the applicable User Agency or Defense Investigative Service and arrange for secure inland shipment within the United States if such shipment has not been prearranged.

e. Transportation plan requirements:

(1) Preparation and coordination:

(a) **Foreign Military Sales**. U.S. classified material to be furnished to a foreign government or international organization under Foreign Military Sales (**FMS**) transactions shall normally be shipped via the Defense Transportation System (**DTS**) and delivered to the foreign government within its own territory. The U.S. Government may permit other arrangements for such shipments when it determines that the recipient foreign government has its own secure facilities and means of shipment from the point of receipt to ultimate destination. In any FMS case, the DoD Component having security cognizance over the classified material involved is responsible, in coordination with the foreign recipient, for developing a transportation plan. When the point of origin is a U.S. contractor facility,

the contractor and Defense Investigative Service will be provided a copy of the plan by the DoD Component.

(b) Commercial Transactions. The contractor shall prepare a transportation plan for each commercial contract, subcontract, or other legally binding arrangement providing for the transfer of classified freight to foreign governments, to be moved by truck, rail, aircraft, or ship. The requirement for a transportation plan applies to U.S. and foreign classified contracts. The Defense Investigative Service will approve transportation plans that support commercial arrangements or foreign classified contracts.

(c) The transportation plan shall describe arrangements for secure shipment of the material from the point of origin to the ultimate destination. It must identify recognized points of embarkation from the United States, its territories, or possessions for transfer to a specified ship, aircraft, or other authorized carrier. It must identify a government or commercial secure facility in the vicinity of the points of embarkation and debarkation that can be used for storage if transfer or onward movement cannot take place immediately. Except as described in subparagraph e(1)(d) below, a U.S. Government official authorized to transfer custody and control must supervise the on-loading of classified material when the material has yet to be officially transferred. The plan must provide for security arrangements in the event custody cannot be transferred promptly.

(d) Upon transfer of title to the purchasing foreign government, classified material may be delivered to a freight forwarder that is designated, in writing, by the foreign government as its representative for that shipment and is cleared to the level of the classified material to be received. The freight forwarder shall be provided a copy of the transportation plan and agree to comply.

(2) The transportation plan shall, as a **minimum**, include:

(a) A description of the material to be shipped and a brief narrative describing where and under what circumstances transfer of custody will occur.

(b) Identification, by name and title, of the designated government representative (or alternate) of the recipient government or international organization who will receipt for and assume security

responsibility for the classified material.

(c) Identification and specific location(s) of delivery point(s) and security arrangements while the material is located at the delivery points.

(d) Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their clearance.

(e) Identification of any storage or processing facilities and transfer points to be used; certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped; and a description of security arrangements while the material is located at the facilities.

(f) Routes and, if applicable, security arrangements for overnight stops or delays enroute.

(g) **Arrangements** for dealing with port security and customs officials.

(h) The identification, by name or title, of couriers, escorts, or other responsible officials (e.g. Captain or Crew Chief) to be used, including social security, government identification, or passport number, security clearance, and details concerning their responsibilities.

(i) Description of the shipping methods to be used and the identification of the foreign or domestic carriers.

(j) Description of packaging requirements, seals and storage during shipment.

(k) A requirement for the recipient government or international organization to examine shipping documents upon receipt of the classified material in its own territory and notify DIS or the DoD Component having security cognizance over the classified material if the material has been transferred enroute to any carrier not authorized by the transportation plan.

(1) Requirement for the recipient government or international organization to inform DIS or the DoD Component having security cognizance over the classified material promptly and fully of any known or suspected compromise of classified material.

(m) Arrangements for return shipments if necessary for repair, modification or maintenance.

APPENDIX I

SPECIAL ACCESS PROGRAM DOCUMENTATION

	<u>Page</u>
Special Access Program Budget Format	I-2
Congressional Notification of SAP Establishment Format	I-3
Special Access Program Summary Report Format	I-4
Special Access Program Quad Chart Format	I-5
Quad Chart Instructions	I-5
Congressional Notification of Change Format	I-7

CONGRESSIONAL NOTIFICATION OF SAP ESTABLISHMENT FORMAT

(CLASSIFICATION)

Honorable Jane S. Able
Chairperson, Committee on (Name of Committee)
House of Representatives
Washington, DC 20515-0000

Dear Ms. Chairperson:

(x/XX) Consistent with Section 119(f) of Title 10, United States Code, this is to notify you that I have approved initiation of the Special Access Program named (Nickname) as proposed by the Secretary of the (Military Department), effective 30 days from receipt of this letter.

(X/XX) This program protects extremely sensitive information related to _____

(U) Funds for this Special Access Program have been approved for obligation no earlier than 30 days after receipt of this letter.

Sincerely,

John P. White

CC:
Honorable John B . Doe
Ranking Minority Member

Classified by: _____
Reason: _____
Declassify on: _____

(CLASSIFICATION)

SPECIAL ACCESS PROGRAM SUMMARY REPORT FORMAT

SPECIAL ACCESS PROGRAM SUMMARY FOR FISCAL YEAR 19XX SUMMARY

IDENTIFICATION: SAP nickname and associated subprogram nicknames.

TYPE: Acquisition, Intelligence, or Operations and Support SAP.

SPONSOR: DoD Component and office of primary responsibility.

OSD POC: **OSD-Level** SAP Central Office and point of contact. (May be an OSD or JCS Office or recommend a OSD point of contact if none has been designated.)

ACCESS: Number of individuals access in the following:

Department of Defense:

Executive Branch outside the Department of Defense:

Congress and Staff

Contractors:

TOTAL:

SPECIAL ACCESS PROGRAM QUAD CHART FORMAT

CLASSIFICATION

<p><i>-GRAPHIC-</i></p>	<p>STATUS - ISSUES</p>																
<p>PROGRAM NICKNAME & DESCRIPTION</p>	<table><tr><th colspan="4">BUDGET & SCHEDULE</th></tr><tr><th>TASK</th><th>FY 97</th><th>FY 98</th><th>FY 99</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td>BUDGET TOTAL</td><td></td><td></td><td></td></tr></table>	BUDGET & SCHEDULE				TASK	FY 97	FY 98	FY 99					BUDGET TOTAL			
BUDGET & SCHEDULE																	
TASK	FY 97	FY 98	FY 99														
BUDGET TOTAL																	

CLASSIFICATION

QUAD CHART INSTRUCTIONS

UPPER LEFT SIDE:

Photo/line drawing/artist sketch of item being developed. If a technology, an illustration of the technology application.
“A picture is worth a thousand words.”

UPPER RIGHT SIDE:

Program status.
Important issues affecting program status of progress.

LOWER LEFT SIDE:

Brief program description. What is it? Where is program going? What need does it fill? Why a SAP?

Highlight major points and successes or problems.

LOWER RIGHT SIDE:

Include current FY and next 2 FYs as a minimum.

Include most recent or next (whichever is closer) milestone or DAB level review.

FY total include all types of \$ (R&D, Procurement, O&M, etc.)

Schedule bars should be accurate to the month if possible.

FORMAT INSTRUCTIONS:

Slide generated using Power Point software

Slide is black background - Words and lines are white unless otherwise specified.

Page setup is 9.4 by 7.4 inches. Box is 9.0X 6.6 inches centered on the page.

All fonts are **VELVETICA**

Classification is red (**RD8**), bolded, 18 point.

Most headings (STATUS-ISSUES, XXX YYY PROGRAM, and BUDGET& SCHEDULE) are bold, 14 point.

Bullets are 85% of character size - color yellow (**YW8**).

Program narrative and issues are 12 point, non-bold.

Budget & Schedule headings are 14 point, non-bold.

Budget & Schedule detail is 12 point, non-bold.

Follow-on slides use the same layout, letter sizes and color scheme except quad chart format are not required.

CONGRESSIONAL NOTIFICATION OF CHANGE FORMAT

(Downgrade classification, remove SAP controls, declassify, or make a public announcement)

(CLASSIFICATION)

Honorable Jane S. Able
Chairperson, Committee on (Name of Committee)
House of Representatives
Washington, DC 20315-0000

Dear Ms. Chairperson:

(x/XX) Consistent with Section 119(c)(1) of Title 10, United States Code, this is to notify you that I have approved the (change in classification/declassification) of the Special Access Program names (Nickname). This program will be (declassified/reclassified) as proposed by the Secretary of (Military Department), effective no earlier than 14 days from the date of this letter. After that date the program will be (unclassified/classified) at the (Classification) level.

(X/XX). Special Access Program (Nickname) is being (declassified/reclassified) because

A public announcement of this change in classification (is/is not) planned. The announcement will take place on or

Sincerely,

John P. White

CC:

Honorable John B. Doe
Ranking Minority Member

Classified by: _____
Reason: • _____
Declassify on: _____

(CLASSIFICATION)